IP SOBRE ATM

GABRIEL RAMÍREZ LABORDE

MARGARITA TINOCO YEPES

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERIAS

DIRECCIÓN DE PROGRAMAS DE INGENIERÍA ELECTRICA Y ELECTRÓNICA

CATAGENA DE INDIAS, D. T. Y C

2004

IP SOBRE ATM

GABRIEL RAMÍREZ LABORDE

MARGARITA TINOCO YEPES

Monografía presentada como registro de aprobación del Minor en Comunicaciones y Redes

Director

EDUARDO GOMEZVASQUEZ

Magíster en Ciencias Computacionales

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERIAS

DIRECCIÓN DE PROGRAMAS DE INGENIERÍA ELECTRICA Y ELECTRÓNICA

CATAGENA DE INDIAS, D. T. Y C

2004

Nota de aceptación

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Cartagena, Junio 7 de 2004

Cartagena, Junio 7 de 2004

Señores

COMITÉ DE REVISIÓN DE MONOGRAFÍA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

La Ciudad

Apreciados señores:

Por medio de la presente nos permitimos informarles que la monografía titulada "**IP SOBRE ATM"** ha sido desarrollada de acuerdo a los objetivos establecidos.

Como autores del proyecto consideramos que el trabajo es satisfactorio y amerita ser presentado para su evaluación.

Atentamente,

GABRIEL RAMÍREZ LABORDE	**MARGARITA TINOCO YEPES**
Código 9604507	Código 9904510

Cartagena, Junio 7 de 2004

Señores

COMITÉ DE REVISIÓN DE MONOGRAFÍA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

La Ciudad

Apreciados señores:

Por medio de la presente me permito informarles que la monografía titulada '**IP SOBRE ATM"** ha sido desarrollada de acuerdo a los objetivos establecidos.

Como director considero que el trabajo es satisfactorio y amerita ser presentado para su evaluación.

Atentamente,

EDUARDO GOMEZ VÀSQUEZ

Magíster en Ciencias Computacionales

AUTORIZACIÓN

Cartagena de Indias D. T. y C

Junio 7 de 2004

Yo GABRIEL RAMÍREZ LABORDE, identificado con la cédula de ciudadanía número 9.102.376 de la ciudad de Cartagena. Autorizo a la Universidad Tecnológica de Bolívar a hacer uso de mi trabajo de grado y publicarlo en el catálogo ON LINE de la Biblioteca.

_____

GABRIEL RAMÍREZ LABORDE

AUTORIZACIÓN

Cartagena de Indias D. T. y C

Junio 7 de 2004

Yo MARGARITA TINOCO YEPES identificado con la cédula de ciudadanía número 45.530.201 de la ciudad de Cartagena. Autorizo a la Universidad Tecnológica de Bolívar a hacer uso de mi trabajo de grado y publicarlo en el catálogo ON LINE de la Biblioteca.

_____

MARGARITA TINOCO YEPES

ARTICULO 105

La Universidad Tecnológica de Bolívar, se reserva el derecho de propiedad intelectual de todos los trabajos de grado aprobados, y no se pueden ser explotados comercialmente sin autorización.

DEDICATORIA

Dedico esta monografía a Díos por darme fuerza para llegar hasta aquí, a mi familia por apoyarme en mis estudios y a mamul por todo ese amor que me brindo a lo largo de este camino.

MARGUI

AGRADECIMIENTOS

Los autores expresan sus agradecimientos a:

A nuestro director **EDUARDO GOMEZ V.**

A nuestro asesor **DAVID SENIOR ELLES.**

Al ingeniero **GONZALO LOPEZ**, por su valiosa ayuda.

A todos los profesores y compañeros que a lo largo de nuestra formación profesional nos brindaron y compartimos sus conocimientos, su amistad, su alegría y apoyo.

Y a todas aquellas personas que colaboraron en alguna para la ejecución de esta monografía.

TABLA DE CONTENIDO

Pág.

LISTA DE FIGURAS

ANEXOS

INTRODUCCIÓN 1

1. Capítulo 1 **8**

1.1. EL PROBLEMA DE INVESTIGACIÓN **8**

1.1.1. Planteamiento del problema 8

1.1.2. Formulación del problema 9

1.2. OBJETIVOS **9**

1.2.1. Objetivo General 9

1.2.2. Objetivos específicos 10

1.3. JUSTIFICACIÓN **11**

2. Capítulo 2 **13**

2.1. IP CLÁSICO SOBRE ATM **13**

2.1.1. Encapsulado de PDU de capa de red 13

2.1.2. Comunicación dentro de la subred LIS 16

2.1.3. Resolución de direcciones 18

2.1.4. Formato de paquetes 25

2.1.5. Prueba de IP clásico sobre ATM 27

2.1.6. Resultado de desempeño 30

2.1.7. Comunicación fuera de la subred LIS 33

2.1.8. Ventajas e inconvenientes del IP clásico 35

3. Capítulo 3 **37**

3.1. EMULACIÓN DE LAN **37**

3.1.1. Arquitectura de Emulación de LAN 40

3.1.2. Operación de la Emulación de LAN 43

3.1.3. Redundancia de LANE 49

3.1.4. Ventajas y Desventajas 52

4. Capítulo 4 **55**

4.1. MPOA (MULTIPROTOCOL OVER ATM) **55**

4.1.1. Introducción 55

4.1.2. Multiprotocolo sobre ATM 59

4.1.3. Tres Elementos Básicos 63

4.1.3.1. LANE 63

4.1.3.2. NHRP 64

4.1.3.3. Enrutador Virtual 65

4.1.4. Componentes Lógicos 66

4.1.5. Cómo Trabaja 69

4.1.6. Ventajas y Desventajas 77

5. Capítulo 5 **78**

5.1. ANÁLISIS TÉCNICO ECONÓMICO Y RELACIÓN COSTO BENEFICIO 78

5.1.1. La gestión financiera del proyecto 78

5.1.2. Relación costo beneficio 79

CONCLUSIONES

BIBLIOGRAFÍA

LISTA DE FIGURAS

Pág.

FIGURA.1 ENCAPSULADO PDU. 13

FIGURA.2 ENCAPSULADO PDU. 14

FIGURA.3 COMUNICACIÓN DENTRO DE LA SUBRED LIS. 17

FIGURA.4 BÚSQUEDA DE LA DIRECCIÓN IP. 20

FIGURA.5 ESTABLECIMIENTO DE UN CANAL VIRTUAL CONMUTADO SVC PARA DATOS IP. 22

FIGURA.6 ENCAPSULADO Y SEGMENTACIÓN DE UN PAQUETE IP A LA SECUENCIA DE CELDAS ATM. 27

FIGURA.7 EMULACIÓN DE DETECTORES DE CELDA. 33

FIGURA.8 COMUNICACIÓN FUERA DE LA SUBRED LIS. 34

FIGURA.9 EMULACIÓN DE REDES LAN. 38

FIGURA.10 EMULACIÓN DE REDES LAN. 39

FIGURA.11 ARQUITECTURA DE LA EMULACIÓN LAN. 42

FIGURA.12 PASOS DE LA INICIALIZACIÓN DE LA UNIÓN DE CLIENTE LEC CON LA RED ELAN. 45

FIGURA.13 OPERACIÓN DEL SERVIDOR DE EMISIÓN DE DIRECCIÓN 47

DESCONOCIDA DE BUS.

FIGURA.14 DIRECCIONAMIENTO Y MAPEO DENTRO DEL ENRUTADOR. 56

FIGURA.15 DIAGRAMA COMPLETO DE MPOA. 58

FIGURA 16 ESTABLECIMIENTO DE UNA CONEXIÓN. 60

FIGURA.17 CONFIGURACIÓN CONSOLIDADA PARA UNA RED ENTERA. 62

FIGURA.18 ENRUTADOR VIRTUAL. 65

FIGURA.19 COMPONENTES LÓGICOS. 66

FIGURA.20 OPERACIÓN BÁSICA DE MPOA. 72

FIGURA.21 CONEXIÓN DIRECTA DE ATAJOS. 73

FIGURA.22 PAQUETE ENVIADO A TRAVÉS DE UNA RED MPOA. 74

FIGURA.23 COEXISTENCIAS Y MIGRACIÓN. 76

LISTA DE ANEXOS

ACRÒNIMOS

ARP Address Resolution Protocol

B-LLI Broadband Low Layer Information

BCOB-C Broadband Bearer Connection Oriented Service Type C

BCOB-X Broadband Bearer Connection Oriented Service Type X

BUS Broadcast and Unknown Server

CIE NHRP Client Information Element

CPCS-PDU Common Part Convergence Sub-layer Protocol Data Unit

DLL Data Link Layer

ELAN Emulated LAN

IE Information Element

IETF Internet Engineering Task Force

InATMARP Inverse ATM Address Resolution Protocol

ION Internetworking Over NBMA (Non-Broadcast Multi-Access)

IP Internet Protocol

IPX Internetwork Packet Exchange

L3 Internetwork Layer

LANE LAN Emulation

LEC LAN Emulation Client

LECS LAN Emulation Configuration Server

LES LAN Emulation Server

LIS Logical IP Subnet

LLC Logical Link Control

MARS Multicast Address Resolution Server

MPC MPOA Client

MPOA Multiprotocol over ATM

MPS MPOA Server

MTU Maximum Transmission Unit

NBMA Non-Broadcast Multi-Access (e.g. ATM, Frame Relay)

NHC Next Hop Client

NHRP Next Hop Resolution Protocol

NHS Next Hop Server

NLSP NetWare Link State Protocol

OSPF Open Shortest Path First

PCR Peak Cell Rate

PDU Protocol Data Unit

QoS Quality of Service

RIP Routing Information Protocol

RSVP Resource Reservation Protocol

SCSP Server Cache Synchronization Protocol

SDU Service Data Unit

SNAP SubNetwork Attachment Point

SVC Switched Virtual Channel Connection

TLV Type-Length-Value Encoding

TTL Time to LiveVCC Virtual Channel Connection

GLOSARIO DE TERMINOS

Aquí presentamos un pequeño diccionario ordenado alfabéticamente y en forma ascendente, relacionado solamente con la terminología utilizada en el presente trabajo con la finalidad de facilitar su lectura y comprensión sin necesidad de recurrir a otros textos especializados o diccionarios, haciendo del presente documento lo más autosuficiente posible.

ANCHO DE BANDA: determina la cantidad de megas que pueden "viajar" en una conexión. Se mide por lo general en bytes o bits por segundo (se podría comparar con una cañería de agua, cuanto más ancha, mayor será la cantidad de fluido se podrá transmitir). Al contratar un proveedor de Internet, debemos tener en claro cual será su ancho de banda, y puede estar comprendido entre 64 Kbps (Kilo bits por segundo), 128 Kbps, 256 Kbps, 1 Mbps (Mega bit por segundo) o 2 Mbps. Todas aquellas respuestas que no contengan uno de estos datos puede significar que no están siendo sinceros. Debemos asegurarnos de cual es la velocidad exacta ya que de esta dependerá nuestra cuenta telefónica. Medida de la cantidad de información que se puede transmitir al mismo tiempo.

ARP: Address Resolution Protocol. Protocolo de resolución de Dirección. Protocolo que traduce las direcciones del protocolo de Internet (IP) en direcciones de red físicas.

ARPANET: red Pionera de conmutación de paquetes (packet switching) desarrollada al inicio de los 70 por la empresa BBN y financiada por ARPA (luego DARPA). ARPANET se convirtió luego en "'Internet." El término ARPANET desapareció oficialmente en 1990.

ATDM. Asynchronous Time Division Multiplexing. Multiplexado asincrónico por división de tiempo. Método de envío de información que emplea el multiplexado usual por división de tiempo (TDM), pero en donde se asignan ranuras de tiempo cuando se requieren, en lugar de preasignarlas a transmisores específicos.

ATM: asyncronous Transmision Mode. Modo de Transmisión Asíncrona. Sistema de transmisión de datos usado en banda ancha para aprovechar al máximo la capacidad de una línea. Se trata de un sistema de conmutación de paquetes que soporta velocidades de hasta 1,2 Gbps.

BANDA ANCHA: un método de transmisión que causa una amplitud de banda mayor que la de un canal de voz, y potencialmente capaz de velocidades de transmisión mucho más altas; también llamada banda amplia.

BANDA BASE: un método de transmisión generalmente para distancias cortas, en el cual toda la amplitud de banda del cable se requiere para transmitir una sola señal digital.

BACKBONE: estructura de transmisión de datos de una red o conjunto de ellas en Internet. Literalmente: "esqueleto". También se denomina así al conjunto de conexiones que forman la base o "eje central" de una red de computadoras.

BIT: Binary Digit. Dígito Binario. Unidad mínima de información, puede tener dos estados "0" o "1".

BUS: camino principal para transmitir señales. Sinónimo de trunk.

BYTE: agrupación básica de información binaria, equivalente a un carácter. Se conoce también por octeto, que es la agrupación mas usual (8 bits mas un bit de paridad). Pero existe también el sexteto. Es la contracción de Binary Term. La memoria principal (RAM, o memoria de acceso aleatorio) y secundaria (correspondiente a los medios de almacenamiento magnéticos) de una computadora se mide en Kilobytes (1.024 bytes), Megabytes (un millón de bytes, o 1.048.576 bytes) o Gigabytes (mil millones de bytes).

BROADCAST, MULTICAST: en la actualidad no hay funciones de broadcast similares a las de las LAN's. Pero sí existe una función de multicast. El término ATM para multicast es "conexión punto - multipunto".

CANAL: medio de transmisión por el cual se difunde una comunicación entre dos usuarios.

CELDAS: todo tipo de información (voz, imágenes, vídeo, datos, etc.) se transporta a través de la red en bloques muy pequeños (48 bytes de datos más una cabecera de 5 bytes) llamados celdas.

CLIENTE / SERVIDOR: el servidor es una simple computadora que ha sido configurada con la aplicación de software adecuada para ofrecer los archivos que sean solicitados. El programa cliente es un browser que muestra los documentos que se seleccionan del WEB. ¿Como se comunica el cliente con el servidor?, a través de un conjunto de reglas llamadas HTTP, Hypertext Transfer Protocol. Por medio de estas reglas se salvan los documentos y se muestran al usuario.

CONMUTACIÓN POR HARDWARE: ATM está diseñado de tal forma que se emplean simples elementos de lógica hardware en cada nodo para realizar la conmutación. En un enlace de 1 Gbps llega una nueva celda, y se transmite una celda cada 0.43 microsegundos. El tiempo de conmutación es mínimo.

DIRECCIONAMIENTO: una dirección ATM de un extremo de la conexión se codifica bien como una dirección de 20 bytes basada en OSI NSAP (utilizada para direccionamiento en redes privadas, con tres formatos posibles) o como una dirección E.164 Public UNI (del estilo de los números telefónicos, usados para redes TM públicas).

ENCAMINAMIENTO: el flujo de información se produce a lo largo de rutas (llamadas "canales virtuales") establecidas como una serie de punteros por la red. La cabecera de una celda contiene un identificador que vincula la celda al camino correcto que debe tomar para llegar a su destino. Las celdas de un canal virtual particular siempre siguen el mismo camino y se entregan en el destino en el mismo orden en el que llegaron al canal.

ETHERNET: es la tecnología de red de área local más extendida en la actualidad. Fue diseñado originalmente por Digital, Intel y Xerox por lo cual, la especificación

original se conoce como Ethernet DIX. Posteriormente en 1.983, fue formalizada por el IEEE como el estándar Ethernet 802.3.

FDDI: fiber Digital Device Interface. Dispositivo Interface de Fibra (óptica) Digital.

FRAME RELAY: protocolo de enlace mediante circuito virtual permanente muy usado para dar conexión directa a Internet.

FTP: file Transfer Protocol. Protocolo de Transferencia de Ficheros. Uno de los protocolos de transferencia de ficheros mas usado en Internet. También, Protocolo para transferir archivos entre máquinas que utilicen TCP/IP. Uno de las maquinas (PC) puede ser nuestra computadora y el otro cualquiera de todos los conectados a la Internet (según su dirección). Condición para ello son también aquí el USER-ID y palabra de paso (password o palabra clave). Una especialidad son los FTP Server anónimos. Estos computadores tienen una parte pública, en la que se encuentran a disposición las diferentes cosas útiles (programas, textos, imágenes, sonidos, etc.) que alcanzan un tamaño de muchos Gigabytes. Para entrar, como User-ID simplemente teclee anónimos y como palabra clave de paso la propia dirección de correo electrónico o e-mail.

FIBRA OPTICA: es el medio de transmisión de datos más moderno y eficaz que existe hasta el momento en el mundo de las telecomunicaciones, capaz de

transmitir mas de un millón de líneas telefónica por segundo con un grado de seguridad de datos absoluto.

HDLC: high-Level Data Link Control. Control de Enlace de Datos de Alto Nivel. Protocolo de enlace adoptado por el CCITT para regular el encuadre de los datos de información manejados en forma remota.

HOST: computador conectado a Internet. Computadoras en general. Computadora central. También, cada uno de los PC's de una red que comparten recursos con otros conectados a la misma.

HTML: hyperText Markup Language. Lenguaje de Marcas de Hypertexto. Lenguaje para elaborar páginas Web actualmente se encuentra en su versión 3. Fue desarrollado en el CERN.

HTTP: hyperText Transfer Protocol. Protocolo de Transferencia de Hypertexto. Protocolo usado en la WWW.

HTML: hyperText Markup Language. Lenguaje de etiquetas de hipertexto. Es el lenguaje mediante el cual se crean y diseñan las páginas Web.

IEEE: institute of Electrical and Electronics Engineers. Instituto de Ingenieros Eléctricos y Electrónicos. Asociación Norteamericana.

IP: internet Protocol. Protocolo de Internet. Bajo este se agrupan los protocolos de Internet. También se refiere a las direcciones de red Internet. Éstas se componen de cuatro bytes (es decir, de números menores de 255) separados por puntos, de la siguiente forma:

xxx.xxx.xxx.xxx por ejemplo: 128.214.6.100

Esta es la llamada dirección IP o número IP (se utiliza durante la transmisión de datos). Pero como es un sistema de identificación difícil de recordar para el usuario, se creó el llamado FQDN (Full Qualified Domain Name o Nombre de Dominio Completo) que hace corresponder a cada dirección IP un nombre similar a las direcciones de correo ordinario. Esto es, se subdivide en los llamados dominios principales (que equivaldrían al país). Por ejemplo, Argentina tiene asignado el dominio ar, España es, y así sucesivamente.

Posteriormente se especifican la organización, la compañía, etc. (por ejemplo, .uba corresponde a la Universidad de Buenos Aires), el centro, etc. Y por último se requiere el nombre del host (que representaría al conjunto de datos formado por la calle, el número, etc.).

En el caso de la dirección 128.214.6.100 que corresponde al nombre ftp.funet.fi, que leído de izquierda a derecha sería: .fi = Finlandia, .funet = Red Finlandesa de Investigación y ftp = al nombre del Host.

Cuando se accede a un host en Internet, se puede especificar tanto su dirección IP, como su nombre. Cualquiera de las dos maneras es válida.

IPX: Internet Packet Exchange. Intercambio de Paquetes entre Redes. Inicialmente protocolo de Novell para el intercambio de información entre aplicaciones en una red Netware.

ISP: Internet Service Provider. Proveedor de Servicios Internet. Divididos en dos grandes grupos: los grandes proveedores (Impsat, Startel, Satlink), que son a su vez dueños de sus propias redes, y los demás. Por supuesto que esos demás no son necesariamente pequeños (Datamarkets, Teletel, AOSLA). Todo ellos, algunos mas y otros menos, además de acceso, desarrollan su propio contenido, incluyendo: Chat, noticias (news), archivos, compras online, referencias de búsqueda, etc. Esto en Argentina.

INTERFAZ DE USUARIO FINAL: la única forma para que un protocolo de nivel superior se comunique sobre una red ATM es por medio de la capa ATM AAL ("ATM Adaptation Layer"). La función de esta capa es realizar el mapeado entre las PDU's y las celdas. Hay cuatro tipos diferentes de AAL, AAL1, AAL2, AAL3/4 Y AAL5. Estos AAL's ofrecen distintos servicios a los protocolos de nivel superior. Aquí se muestran las características de AAL5, usado para TCP/IP:

- Modo mensaje y modo flujo
- Entrega garantizada
- Entrega no garantizada(usada por TCP/IP)
- Fragmentación de los datos en bloques y segmentos
- Operación multipunto

AAl5 proporciona las mismas funciones que una LAN en el nivel MAC ("Medium Access Control"). Los extremos del VC saben el tipo de AAL por medio del mecanismo de configuración de la celda, por lo que la cabecera de la celda no ha de llevarlo. Para los PVC's el tipo AAL se configura administrativamente en los extremos cuando se establece la conexión. Para los SVC's, el tipo de AAL se comunica por el canal vía 0.93B como parte de la solicitud de establecimiento y definición de la conexión y los extremos usan las señales de control para configurarse. Los conmutadores ATM no suelen preocuparse del tipo de AAL de los VC's. El formato AAL5 especifica un formato de paquete con un tamaño

máximo de 64KB - 1 byte de usuario. Las "primitivas" que ha de usar el protocolo de nivel superior como interfaz con la capa AAL (en el SAP de AAL ("Service Access Point") están definidas rigurosamente. Cuando un protocolo de nivel superior envía datos, estos son procesados primero por la capa de adaptación, luego por ATM y por último la capa física se encarga de enviar los datos por la red ATM. Las celdas se transportan y las recibe el otro extremo de la conexión en su capa física, que las pasa a ATM, que tras procesarlas las pasa al AAL receptor, que a su vez devuelve los datos al nivel superior. La función total que ha realizado la red ATM ha sido un transporte no garantizado de información (se podría haber perdido una parte). Desde un punto de vista más conservador del proceso de datos, todo lo que ha hecho la red ATM ha sido sustituir un enlace físico por otro tipo de conexión física - todos los protocolos de alto nivel siguen teniendo que efectuarse (por ejemplo IEEE 802.2).

LAN: local Area Network. Red de Área Local. Red de computadoras de reducidas dimensiones. Por ejemplo una red distribuida en una planta de un edificio. Sistema que conecta a dos o más computadoras personales para que puedan comunicarse o utilizar recursos compartidos (compartir: impresoras, acceso a Internet, unidades de CD-ROM, etc.).

MAN: metropolitan Area Network. Red de área Metropolitana.

PAQUETE: cantidad mínima de datos que se transmite en una red o entre dispositivos. Tiene una estructura y longitud distinta según el protocolo al que pertenezca. También llamado TRAMA.

PDH: jerarquía digital plesiocrónica.

PING: packet Internet Gropher. Rastreador de Paquetes Internet. Programa utilizado para comprobar si un Host esta disponible. Envía paquetes de control para comprobar si el host esta activo y los devuelve.

PPP: Point to Point Protocol. Protocolo Punto a Punto. Protocolo Internet para establecer enlace entre dos puntos.

PROTOCOLO: serie de normas o especificaciones técnicas para las comunicaciones vía puerto serial (serie). Los protocolos soportados en los módems pueden variar de uno a otro.

PROVEEDOR DE ACCESO: centro servidor que da acceso lógico a Internet, es decir sirve de pasarela (Gateway) entre el usuario final e Internet.

PROVEEDOR DE CONEXIÓN: entidad que proporciona y gestiona enlace físico a Internet. Por ejemplo Telefónica o Telecom (en Argentina).

PROVEEDOR O PROVIDER: empresa que nos ofrece sus servicios de acceso a Internet; si comparamos a Internet con una autopista, se correspondería con los puestos de peaje. Pueden ser Universidades u oferentes comerciales como Compuserve, America Online, etc. Estos proveedores cobran una cuota generalmente mensual según el tiempo contratado o especificado que puede variar desde 8 horas de conexión hasta el servicio Full o Plano en el cual no hay límites de tiempo (la cuenta telefónica va aparte).

PVC: permanent Virtual Circuit. Circuito Virtual Permanente. Línea punto a punto virtual establecida normalmente mediante conmutaciones de carácter permanente. Es decir a través de un circuito establecido.

QoS: calidad de servicios.

RARP: reverse Address Resolution Protocol. Protocolo de Resolución de Dirección de retorno. Protocolo de bajo nivel para la asignación de direcciones IP a maquinas simples desde un servidor en una red física.

RED: conjunto de computadores conectados con la finalidad de compartir recursos de software y Hardware.

RIP: routing Information Protocol. Protocolo de Información de Routing.

ROUTER: dispositivo conectado a dos o más redes que se encarga únicamente de tareas de comunicaciones.

RFC's: request for comments.

SDH: jerarquía digital síncrona.

SOFTWARE: es todo lo volátil, en contraposición con b que significa hardware. Así se denominan a todos los programas de computación, incluyendo los sistemas operativos. Los jueguitos, las aplicaciones (procesadores de texto, base de datos, planillas de cálculo, graficadores, programas a medida, etc.), sistemas operativos (Windows, Unix, DOS, Linux, etc.), Lenguajes de programación (Visual Basic, Delphi, C++, Pascal, etc.).

SMTP: simple Mail Protocol, protocolo sencillo de transferencia de correo. Protocolo utilizado para el intercambio de mensajes de correo entre estaciones servidores. Para recoger los mensajes se utiliza el protocolo POP3.

SERVIDORES: son las máquinas que se encargan de administrar todos los recursos con los que cuenta la red, tales como: el sistema operativo, paquetes de cómputo, programas de aplicación, información, intercambio de la misma, etc.

SVC: circuito virtual conmutado.

TCP/IP: transmision Control Protocol / Internet Protocol. Es un protocolo mediante el cual se comunican unas PC's con otras en Internet y es independiente de la plataforma. Es decir, puede funcionar en cualquier computadora, de manera que un AMIGA puede comunicarse (cambiar datos) con una compatible PC. También se puede utilizar en redes locales. Las redes locales (LANs) que funcionan con este protocolo reciben el nombre de Intranet. Este protocolo es un poco más complicado de configurar pero es el más potente de todos. No viene cargado por defecto así que tendremos que agregarlo manualmente. Para configurar el TCP/IP hay que conocer un poco el funcionamiento del protocolo. Cada maquina dentro de una red TCP/IP tiene asignado un identificador llamado Dirección IP formado por 4 números separados por puntos (i.e. 194.147.2.100). Para comunicarnos con otra maquina en la red utilizamos su dirección. Como es muy difícil recordar direcciones de este tipo se decidió llamar a los ordenadores con nombres del tipo URL (i.e. www.microsoft.com) y utilizar una maquina con una tabla de tal manera que convierta URL's en Direcciones IP, esta maquina recibe el nombre de DNS. Obviamente no podemos conectarnos a la maquina DNS por su nombre URL sino que tenemos que indicar la Dirección IP del DNS para poder contactar con el. Internet es una gran red TCP/IP donde cada ordenador tiene una dirección IP única, existen otras redes TCP/IP independientes de la Internet como Infovía. Además podemos crearnos nuestra propia red TCP/IP, las llamadas Intranets.

TOKEN RING: red de anillo. Tipo de LAN en el que los computadores de la red están enlazados en forma de anillo y cada uno de ellos (los PC's o nodos) está en continuo contacto con el siguiente.

TOPOLOGY: descripción de los ordenadores de una red y los enlaces entre ellos.

UDP: protocolo perteneciente a TCP/IP. Sustituye a TCP/IP cuando toda la información que se quiere mandar cabe en un solo paquete. Es muy rápido para hacer emisiones unilaterales de vídeo o audio.

VIRTUAL: que no existe físicamente sino solo en software. Simulación. Ejemplo: Virtual Machine, simulación del funcionamiento de un ordenador.

VC: canal virtual.

WAN: wide Area Network. Red de Área Extensa. Red de comunicación de datos que cubre una amplia zona geográfica, como puede ser una Universidad, varios edificios, varias oficinas, secciones, una empresa, hasta todo un país y aún más.

WEB: la red de redes. Así se le dice generalmente a la Internet.

X25: protocolo de transmisión de datos muy usado en Iberpac. Establece circuitos virtuales, enlaces y canales. También: Recomendación del CCITT que define un sistema de almacenamiento y expedición por conmutación de paquetes de la información en una red digital tipo WAN.

XDSL: tecnología que permite a los módems comunicarse a altas velocidades utilizando el cable telefónico, velocidades necesarias para transmisión de datos multimedia.

INTRODUCCIÓN

Para comprender la filosofía de ATM es importante recordar que esta tecnología fue creada con la finalidad de optimizar el uso de las redes telefónicas convencionales aplicando técnicas ya aplicadas en la transmisión de datos; por ejemplo la supresión de silencios empleada en ATM es consecuencia de la aplicación a la voz digitalizada del principio de la conmutación de paquetes que ya se empleaba en X.25 o Frame Relay.

Por su concepción inicial ATM fue desarrollada para aplicarse en redes de área extensa, utilizando como medio de transporte sobre todo SDH (jerarquía digital síncrona), y en menor medida PDH (jerarquía digital plesiocrónica).

Un objetivo de diseño de ATM fue el tráfico multimedia (entendiendo por éste el que comprende voz, vídeo y datos) suministrando diversos niveles de Calidad de Servicio (QoS) en función de las necesidades planteadas por la aplicación.

El tamaño de celda elegido (48 bytes y 5 de cabecera) fue un compromiso adoptado tras largas discusiones entre los operadores americanos y los europeos. Los primeros preferían celdas grandes para reducir el overhead de la cabecera, mientras que los segundos querían celdas pequeñas para reducir el retardo de paquetización y así no tener que instalar dispositivos canceladores de eco en la red.

A diferencia de ATM, que nació a partir de las compañías telefónicas, TCP/IP fueron protocolos creados por informáticos con la única finalidad de permitir una transmisión de datos eficiente sobre todo tipo de medios físicos. La interoperabilidad era un aspecto fundamental del diseño, y la Calidad de Servicio no estaba dentro de los planes iniciales (aunque posteriormente se han incorporado diversas mejoras en este sentido).

Para conseguir un uso eficiente de la infraestructura el tamaño de los paquetes (llamados datagramas) es variable, con un valor máximo de 64 Kbytes.

Es curioso comparar, siquiera sea brevemente, la evolución histórica de TCP/IP y ATM. ARPANET, precursora de Internet, empezó a funcionar en 1969, y los protocolos TCP/IP se inventaron en 1974. El verdadero desarrollo de TCP/IP empezó en 1984 con la creación de NSFNET. Entretanto la antecesora de ATM fue la red denominada Spider que entró en funcionamiento en 1972. Hacia mediados de los 80 la CCITT proponía el concepto de red ISDN de banda ancha (B-ISDN), y a finales de la década se decidió utilizar como base para dicha red la tecnología ATDM (Asynchronous Time Division Multiplexing), rebautizada entonces a ATM.

Como consecuencia de su origen tan distinto las filosofías de ATM e IP difieren en muchos aspectos sustanciales. El mas importante es el funcionamiento orientado a conexión de ATM y el no orientado a conexión de IP; de aquí se derivan

diferencias tales como el respetar (ATM) o no (IP) el orden de envío de las celdas (o los paquetes).

También como consecuencia de esto en ATM es mucho mas sencillo ofrecer diversos niveles garantizados de Calidad de Servicio, mientras que en IP el servicio que se ofrece normalmente no es garantizado, sino del tipo denominado 'best effort' (mejor esfuerzo).

Existen diversas organizaciones implicadas en el proceso de estandarización de ATM.

La más importante es el Sector de Estándares de Telecomunicaciones de la Unión Internacional de Telecomunicaciones, también llamado ITU-T (conocido hasta el año 1993 por las siglas CCITT). Los principales estándares de interés son los denominados I.320 e I.360.

Dado que el proceso de estandarización de la ITU-T es necesariamente lento y complejo y no permite responder con suficiente rapidez a las demandas del mercado, se ha creado un consorcio de fabricantes denominado ATM Forum que define sus propios estándares. Actualmente el Forum ATM tiene más de 800 miembros, entre los que se encuentran fabricantes, operadores y usuarios.

También son de especial importancia, sobre todo hablando del transporte de IP sobre ATM, las especificaciones del IETF (Internet Engineering Task Force) que se publican en los documentos conocidos como RFC's (Request For Comments).

Otras organizaciones tienen relación con el mundo ATM en temas concretos, pro ejemplo el DAVIC (Digital Audio Visual Council) que se ocupa de estandarizar

sistemas de distribución de vídeo a nivel residencial. Otros casos son el IEEE 802.14 y el Forum ADSL; en ambos se contempla el uso de ATM.

La forma más sencilla de utilizar una red ATM para transportar tráfico IP es utilizar el VC (Canal Virtual) como si se tratara de una línea dedicada. Para incorporar el soporte multiprotocolo se pueden adoptar dos estrategias (ambas definidas por el IETF en el RFC 1483):

- Dedicar un VC diferente para cada protocolo; esto es lo que se denomina Multiplexado por VC.
- Dedicar un solo VC y diferenciar el protocolo mediante una cabecera 802.2 LLC/SNAP, de forma análoga a lo que se hace en las redes locales.

La elección de una u otra técnica vendrá condicionada normalmente por el tipo de servicio o contrato. Si el establecimiento de VC's no tiene costo normalmente será preferible realizar multiplexado por VC's, ya que así evitaremos el overhead de la cabecera 802.2. En cambio, si el establecimiento de un VC o la asignación de caudal tienen costo, utilizaremos preferentemente encapsulado 802.2, ya que así podremos agrupar y reducir costos, aprovechando mejor los recursos disponibles.

En ambos casos la correspondencia entre direcciones ATM e IP se realiza a través de tablas de forma manual. Dado que esto se utilizará normalmente en entornos donde se empleen Canales Virtuales Permanentes (PVC's) esto no suele ser un problema.

En un mayor nivel de sofisticación respecto al anterior podemos situar la técnica denominada ‘Classical IP over ATM’, que básicamente hace uso del soporte multiprotocolo RFC 1483 ya descrito y de ATMARP, un mecanismo que permite la traducción automática de direcciones ATM a IP contenido en el RFC 2225 (que ha sustituido al original RFC 1577).

El uso de RFC 2225 requiere la posibilidad de establecer canales virtuales conmutados (SVC’s), opción que no está normalmente disponible en los servicios ATM actualmente ofrecidos por los operadores. Por tanto en la práctica esta opción solo es viable en redes locales o en redes de área extensa cuando toda la infraestructura ATM es gestionada por el usuario.

En Classical IP over ATM se contempla la segmentación de la red en otras de menor tamaño, creando las denominadas LIS (Logical IP Subnet). Esto es interesante por motivos de seguridad y eficiencia, en particular para poder reducir o limitar el tráfico broadcast.

En el caso de protocolos distintos de IP el IETF no ha definido un mecanismo equivalente al recogido en RFC 2225 para su traducción automática en direcciones ATM. Por tanto en estos casos es necesario crear (y mantener) manualmente tablas de búsqueda de direcciones.

El Classical IP over ATM tiene por su parte la ventaja de tener un overhead más reducido, ya que se evita el encapsulado propio del subnivel MAC (Ethernet o Token Ring). También podemos considerar la tecnología como probada y fiable.

Entre los inconvenientes aparecen los siguientes:

- La ausencia de un mecanismo automático que dinámicamente traduzca las direcciones de otros protocolos diferentes a IP.
- La no integración con Lanas clásicas. Por ejemplo la comunicación entre un host que utilice 'Classical IP over ATM' con uno que utilice LANE o que esté conectado a una red local siempre requerirá el empleo de un router.
- La ausencia de QoS. Esto es consecuencia del tráfico tipo UBR utilizado por Classical IP over ATM.
- El costo cuando se compara con otras alternativas, en particular Fast Ethernet y Gigabit Ethernet

Actualmente, IP es la solución que destaca a la hora de proporcionar servicios a través de Internet. Esto supone que con unos adecuados cambios tecnológicos podrá fortalecer hasta convertirse en los cimientos que asienten la transferencia de datos a través de Internet, permitiendo la difusión de servicios avanzados en el tiempo real y de respuesta prioritaria, entre

- Proyectos de Teleformación y Aula virtual interactiva.
- Servicios avanzados de atención médica y hospitalaria. Telemedicina, teleasistencia o telecirugía.

- video a la carta, multidifusiones, servicios multimedia interactivos o Telespectáculos.
- Transmisión de voz a través de Internet y la construcción de redes privadas virtuales (VPN's).
- Servicios de calidad para voz y fax sobre IP.

Estos servicios exigirán una serie de necesidades crecientes para los ISP y carriers que deberán incorporar a sus redes troncales mecanismos para mantener un control sobre el tráfico, una gestión de recursos, un ancho de banda disponible, así como una adecuada calidad de servicio *(QoS).*

A su vez, los avances en las tecnologías de transporte basadas en switching, encabezadas por la tecnología ATM, proporcionan alta velocidad, calidad de servicio y facilitan la gestión de los recursos en la red, que hemos comentado anteriormente. Comprobando cómo el protocolo de Internet actual, IP, puede beneficiarse de las características que aportan estas nuevas tecnologías parece claro buscar soluciones para conseguir un escenario de integración

IP-ATM. El principal objetivo, por tanto, de este trabajo es analizar y dar a conocer las soluciones que existen actualmente al problema de integrar tráfico IP dentro de la tecnología ATM;

Capítulo 1

1.1. EL PROBLEMA DE INVESTIGACIÓN

1.1.1. Planteamiento del problema

Actualmente los avances tecnológicos han provocado un crecimiento exponencial en los sistemas de cómputo y de telecomunicaciones; el procesamiento y la transmisión de datos han alcanzado niveles inimaginables por nuestros antepasados, al mismo tiempo los usuarios han comenzado a exigir el máximo desempeño de los ya mencionados sistemas mediante los requerimientos de mayor ancho de banda, eficiencia, rendimiento, etc. es decir Calidad de servicio, muchos de las infraestructuras instaladas son obsoletas y no tienen la capacidad para el manejo y la gestión de semejantes volúmenes de información.

Lo anterior ha generado dificultades en diversos campos de la vida actual. A su vez los lineamientos de la sociedad informática contemporánea han convertido al ser humano en un ser dependiente de los sistemas de computo y las tecnologías asociadas; la necesidad de intercambio y consecución de información se ven truncadas por el bajo perfil de nuestros entornos tecnológicos.

Se hace necesario considerar a las redes de banda ancha, como una infraestructura primordial para alcanzar las metas sociales, económicas y

científicas. Los problemas generados por la heterogeneidad del gran número de redes de cómputo y telecomunicaciones existentes nos motivan a plantear el estudio de nuevos mecanismos que favorezcan la homogenización de los sistemas de transporte de datos; bajo este marco aparecen dos tecnologías (IP/ATM), que logrando la sinergia de lo mejor de cada una de ellas y trabajando en sus respectivas debilidades, brinda una alternativa de desarrollo social, económico y científico.

1.1.2. Formulación del problema

¿Cuáles deben de ser las herramientas y recursos mínimos necesarios que deberán ser considerados para el análisis entre tráfico IP y redes ATM en el mundo y así poder disponer de una plataforma que nos facilite la gestión de los recursos en la red en forma eficiente, y los distintos mecanismos para que puedan ser utilizados?

1.2. OBJETIVOS

1.2.1. Objetivo General

Analizar la convergencia IP/ATM y la incidencia del proceso de migración a redes multimedia, mediante la investigación de los avances tecnológicos y

la constitución de un modelo de capas que conlleva a la integración de las tecnologías ATM con las redes IP, para determinar la potencialidad de IP sobre ATM como la solución tecnológica más probable, capaz de producir la homogeneidad de entornos y señalizaciones, así como la simplificación del internetworking, la gestión de redes y sistemas de telecomunicaciones.

1.2.2. Objetivos específicos

Conocer las soluciones que existen actualmente al problema de la integración del tráfico IP en la tecnología ATM, específicamente en IP clásico sobre ATM, Emulación de LAN y MPOA (Multiprotocol Over ATM), basándonos en el estudio de un modelo de capas.

Identificar los pros y los contras de las tecnologías IP sobre ATM en LAN (Local Area Network) y WAN (Wide Area Network).

Establecer una relación coste-beneficio en la integración IP/ATM.

Brindar una visión futura de las redes con tecnología ATM como solución tecnológica altamente viable.

1.3. JUSTIFICACIÓN

Hablar de IP sobre ATM, es, con gran certeza vislumbrar la solución a la evolución de los servicios de telecomunicación y redes computacionales. Los factores que nos llevan a realizar tal afirmación se pueden enmarcar dentro de los siguientes contextos. Primero, la necesidad progresiva de integración de servicios, ligada a la migración hacia tecnologías de mayor exigencia (Banda Ancha); segundo, los requerimientos de altos niveles de desempeño (QoS, Calidad de Servicio) por parte de los usuarios de los sistemas. Los requerimientos anteriores hacen que sea indiscutible la necesidad de definir y dar a conocer las diversas herramientas tecnológicas que garanticen de manera eficaz e individualizada la calidad exigida por cada servicio.

La definición de los marcos que se contemplan en la provisión de QoS, se propone la utilización de IP sobre ATM, de manera que se aprovechen los avances en las tecnologías de transporte basadas en la conmutación, las cuales son liderados por ATM, que proporciona altas velocidades, control sobre los parámetros de QoS y gestión de recursos en la red, de modo que IP resulte beneficiado por las características de la ya mencionada tecnología, aportando su gran popularidad y capacidad de conectividad.

Se debe tener muy en cuenta que IP y ATM, son tecnologías con diferentes orígenes autores y promotores, ATM fue definido por la ITU-T (Unión Internacional de Telecomunicaciones), como el modo de transferencia elegido para brindar soporte a la Red Digital de Servicios Integrados de banda ancha

(B-ISDN), mientras que IP proviene del mundo de las redes computacionales; hechas las correspondientes salvedades reafirmamos la necesidad de un escenario de integración y coexistencia, por lo menos durante algunos años entre IP y ATM, no como tecnologías excluyentes, sino como la sinergia hacia el desarrollo de la comunidad mundial.

Capítulo 2

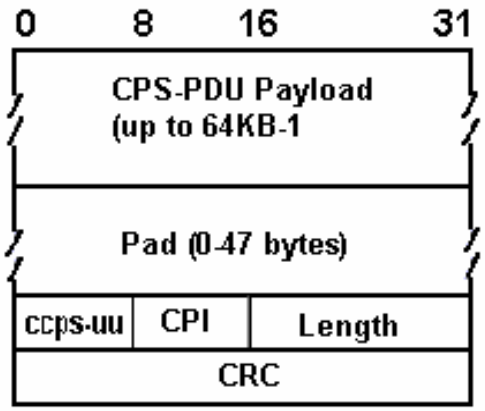
2.1 IP Clásico sobre ATM

La arquitectura ATM difiere significativamente de la arquitectura IP. La primera es una arquitectura no orientada a conexión mientras que la segunda lo es, es decir; es orientada a conexión. Además, el esquema de direcciones es totalmente diferente, al igual que lo es el modelo de comunicación multicast o multienvío. Estas son algunas de las diferencias entre ambos modelos.

2.1.1 Encapsulado PDU de capa de red

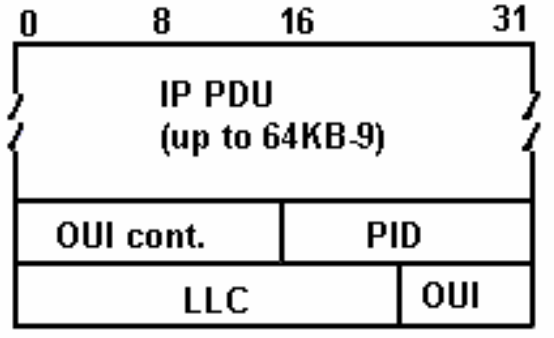
La PDU de TCP/IP se encapsula en una cabecera IEEE 802.2 LLC seguida de una cabecera IEEE 802.1a SNAP (“Sunbnetwork Attachment Point) transportada dentro del campo de carga útil (“payload field”) de una PDU AAL5 CPCS (“Common Part Convergence Sublayer”). El formato de la PDU AAL5 CPCS se muestra en la figura 1.

Fig. 1 Encapsulado PDU



CPCS-PDU Payload

Fig.2 Encapsulado PDU



PAD: Se utiliza como relleno para que el tamaño de CDCS se ajuste a las celdas ATM.

CPCS-UU: El campo CPCS-UU (“User-to-user identification”) se usa para transmitir de forma transparente información de usuario a usuario. Este campo no tiene utilidad en la encapsulación y se le puede dar cualquier valor.

CPI El campo CPI ("Common Part Indicator") alinea la cola del CPCS a 64 bits.

Length, El campo Length indica la longitud, en bytes, del campo Payload. El valor máximo es 65535(64KB - 1).

CRC El campo CRC protege todo el CPCS exceptuándose así mismo.

IP PDU: Dat IP normal comenzando con la cabecera IP.

LLC: Cabecera LLC de 3 bytes con el formato DSAP-SSAP-Ctrl. Para datos IP se pone a 0xAA-AA-03 para indicar la presencia de una cabecera SNAP. El campo Ctrl tiene siempre el valor 0x03 especificando una PDU de tipo "Unnumbered Information Command".

OUI: El campo de 3 bytes OUI ("Organizationally Unique Identifier") identifica una organización que administra el significado del PID (explicado a continuación). Para especificar el tipo EtherType en el PID el OUI tiene que ponerse a 0x00-00-00.

PID: El PID ("Protocol Identifier") de 2 bytes el tipo de protocolo de la PDU que le sucede. Para datagramas IP, el PID es 0x08-00.

El tamaño por defecto de la MTU para miembros IP de la red ATM se discute en el RFC 1626 [1] y se fija a 9180 bytes. La cabecera LLC/SNAP es de 8 bytes; por consiguiente, el tamaño por defecto de la PDU ATM AAL5 es de 9188 bytes. Se puede cambiar el tamaño de la MTU, pero debe hacerse por igual para todos los miembros del LIS. El RFC 1755 [2] recomienda que todas las implementaciones soporten tamaños de MTU de hasta 64KB, inclusive.

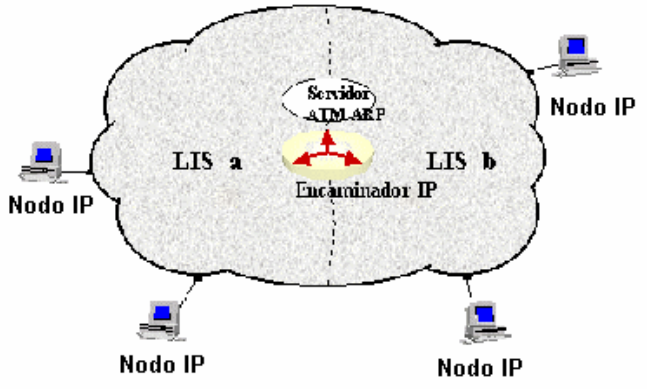
No hay forma de mapear direcciones IP de broadcast o de multicast a ATM. Sin embargo, no hay restricciones para transmitir o recibir datagramas especificando cualquiera de las cuatro direcciones de broadcast estándar de IP descritas en el RFC 1122 [3]. Los miembros, al recibir un broadcast IP para su LIS, deben procesar el paquete como si fuera para ellos.

2.1.2 Comunicación dentro de la subred LIS

En el modelo clásico los nodos IP pueden comunicarse entre sí, si pertenecen a la misma subred IP lógica (LIS, Logical IP Subnet). Una LIS es simplemente un conjunto de hosts y encaminadores conectados a través de una red ATM. Dichos hosts y encaminadores están en una red IP, por lo que comparten la misma dirección de subred.

Si un dispositivo en una LIS se quiere comunicar con otro que esté en otra LIS distinta, debe hacerlo a través de un encaminador que comunique ambas LIS's (no podrán establecer un único circuito virtual para comunicarse).

Fig. 3 Comunicación dentro de la subred LIS



Para que dos dispositivos que están en la misma LIS se puedan comunicar, es necesario que conozcan sus direcciones ATM [4]. Para tal cosa es necesario disponer de un servidor ARP [5] (Address Resolution Protocol). En redes convencionales como las redes Ethernet, los dispositivos IP aprenden sus respectivas direcciones gracias al protocolo ARP que se apoya en la difusión del nivel de enlace. Como las redes ATM carecen de esto se necesita el mencionado servidor para hacer la conversión de direcciones IP a direcciones ATM. Los dispositivos registran en dicho servidor su dirección ATM y su dirección IP de tal forma que cuando un dispositivo se quiere comunicar con otro que está en la misma LIS le solicita al servidor que haga la traducción de la dirección IP a la dirección ATM. Con la dirección ATM ya podrá comunicarse estableciendo un circuito virtual.

2.1.3 Resolución de direcciones (ATMARP y InATMARP)

La resolución de direcciones en una subred lógica IP de ATM la hace el ATMARP ("ATM Address Resolution Protocol") basado en el RFC 826 [6] y en el InATMARP ("Inverse ATM Address Resolution Protocol") basado en el RFC 1293 [7]. ATMARP es el mismo protocolo que ARP pero con las extensiones necesarias para que ARP funcione en el entorno de servidor unicast de ATM. InATMARP es el mismo protocolo que el InARP original, pero aplicado a redes ATM. El uso de estos protocolos difiere en si se utilizan o no PVC's o SVC's.

Tanto ATMARP como InATMARP están definidos en el RFC 1577 [8], que es una propuesta de estándar con estado electivo.

La encapsulación de las peticiones/respuestas de InATMARP y ATMARP se describe mas adelante.

InATMARP

El protocolo ARP se usa para calcular la dirección hardware de un host a partir de su dirección IP. El protocolo InATMARP se usa para calcular la dirección IP de un host a partir de su dirección hardware. En un entorno

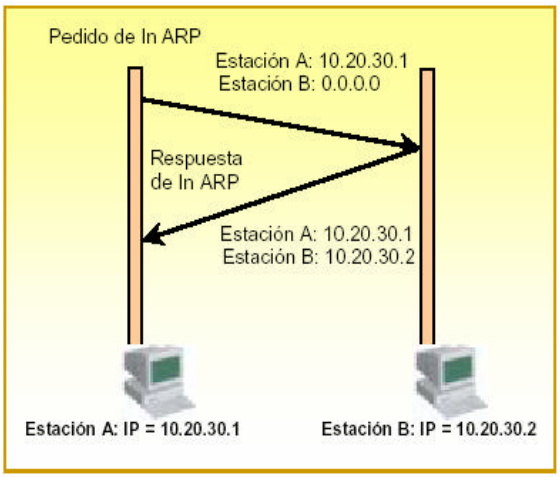
conmutado, primero se establece una VC ("Virtual Connection") o una PVC ("Permanent Virtual Connection") o una SVC ("Switched Virtual Connection") para comunicar con otra estación. Por lo tanto, se sabe la dirección hardware del otro host, pero no la dirección IP. InATMARP proporciona resolución dinámica de direcciones. Utiliza el mismo formato de trama que el ARP estándar, pero define dos nuevos códigos de operación:

- InARP request=8
- InARP reply=9

El InATMARP básico opera esencialmente del mismo modo que ARP, con la excepción de que no hace las peticiones con broadcasts. Esto se debe a que la dirección hardware ya se conoce. Una estación solicitante simplemente formatea una petición insertando sus direcciones hardware de IP (fuente) y la dirección hardware del destino. Luego rellena con ceros el campo de dirección IP del destino y envía el mensaje a la estación de destino. Para cada petición InATMARP, la estación receptora formatea una respuesta utilizando la dirección fuente de la petición como dirección de destino para la respuesta. Ambos extremos actualizan sus tablas ARP. El valor *tipo de hardware* para ATM es el 19 decimal y el campo *EtherType* se pone a 0x806, que indica ARP según el RFC 1700.

En un ambiente de **conexión virtual permanente** (PVC) se usa una configuración manual para establecer los canales virtuales entre cada par de estaciones dentro de la subred lógica LIS. Cada estación usa el protocolo con capacidad de dirección inversa InATMARP para determinar a cual dirección IP está conectada. Se envía un mensaje de pedido con la dirección del IP de la estación A: El mensaje de respuesta contiene la dirección IP del receptor B. La figura 4 muestra la operación del protocolo InATMARP sobre conexiones virtuales permanentes.

Fig. 4 Busqueda de dirección IP

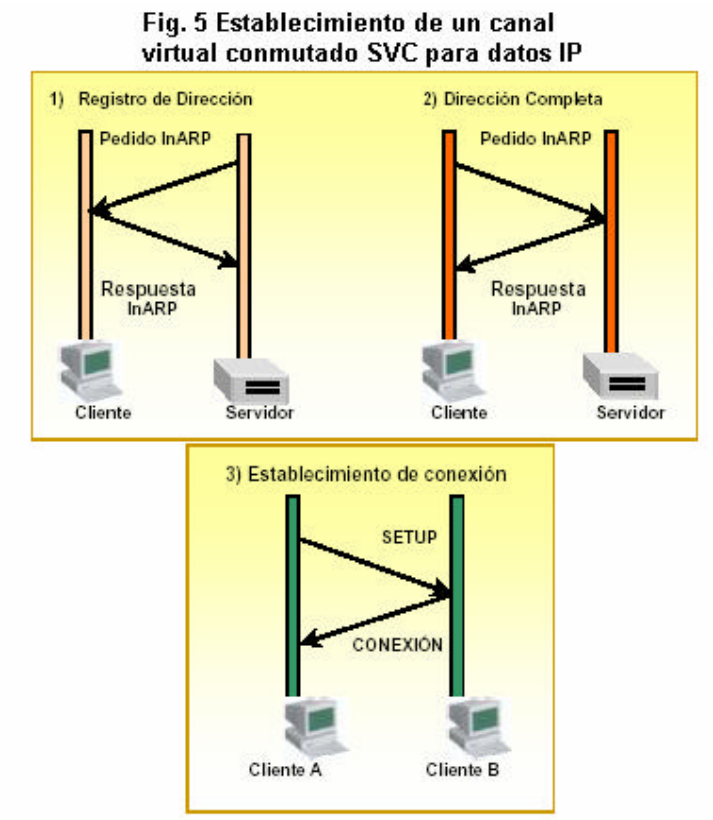


En un ambiente **de conexión virtual conmutada (SVC),** la señalización de la interfaz de usuario con la red conmutada establece los canales virtuales entre las estaciones A y B. Un servidor ATMARP se usa para manejar la tabla de ATM y el par de direcciones I P para cada estación en la subred lógica LIS. Este servidor se localiza en una dirección ATM bien conocida,

que se configura manualmente con cada estación cliente de la subred LIS. Cuando un cliente A establece una conexión al servidor ATMARP, el servidor emite un pedido (request) para determinar la dirección IP del cliente A. Este servidor usa la respuesta (reply) para construir y validar su tabla de direcciones. Si el cliente A necesita enviar un paquete al cliente B, y si A no tiene dirección ATM de B, entonces A debe enviar un pedido ATMARP al servidor, el cual envía la dirección ATM de B como respuesta. Entonces el cliente A utiliza esta dirección para crear el camino virtual usando el mensaje de señalización SETUP. La figura 5 ilustra estos tres pasos para el establecimiento de una conexión virtual conmutada. El cliente A no siempre tiene que preguntar la dirección de B al servidor, si tiene un canal virtual VC abierto hacia B, o si tiene su propia tabla de direcciones construida en base a respuestas anteriores dadas por el servidor. Las entradas en la tabla de direcciones del servidor son invalidadas si la conexión ha sido cerrada por más de 20 minutos.

Las conexiones abiertas son revalidadas enviando pedidos InATMARP en el canal virtual cada 20minutos.

Fig. 5 Establecimiento de un canal virtual conmutado SVC para datos IP



Nota. El servidor ATMARP requiere que cada cliente sea configurado administrativamente con la dirección ATM del servidor ATMARP.

- Si el servidor ATMARP recibe una nueva dirección IP en una respuesta InATMARP la dirección IP se añade a la tabla ATMARP.
- Si la dirección IP de la respuesta InATMARP duplica una dirección IP de una entrada de la tabla y la dirección InATMARP de ATM no coincide la dirección ATM de esa entrada en la tabla y existe un VC abierto asociado a esa entrada, la información InATMARP se desecha y no se hacen cambios en la tabla.

Cuando el servidor recibe una petición ATMARP sobre un VC, en el que la dirección IP y ATM de la fuente coinciden con la asociación que ya existe en la tabla, y la dirección ATM coincide con la que está asociada al VC, el servidor actualiza el time out de la entrada en su tabla para la fuente. Por ejemplo, si el cliente está enviando solicitudes ATMARP al servidor sobre el mismo VC usado para registrarse, el servidor se da cuenta de que ese cliente sigue "vivo" y actualiza su time out en la tabla.

Cuando el servidor recibe un ARP_REQUEST sobre un VC, examina la fuente de la información. Si no hay ninguna dirección IP asociada a ese VC y si la dirección IP de la fuente no está asociada a ninguna otra conexión, entonces el servidor añade esa estación a su tabla. Este no es el procedimiento normal ya que, como se indica arriba, es responsabilidad del cliente registrarse en el servidor ATMARP.

Las entradas de la tabla ATMARP son válidas:

- En clientes por un máximo de 15 minutos
- En servidor por una mínimo de 20 minutos

Antes de invalidar una entrada de su tabla, el servidor ATPARP genera un InARP_REQUEST para cualquier VC abierto asociado con esa entrada y decide lo que ha de hacer de acuerdo con las siguientes reglas:

- Si se recibe una respuesta InARP_REPLY, la entrada en la tabla se actualiza en vez de borrarse.
- Si no hay ningún VC asociado a esa entrada, la entrada se borra.

Por tanto, si el cliente no mantiene un VC abierto al servidor, debe refrescar su información ATMARP en el servidor al menos cada 20 minutos. Esto se hace abriendo un VC al servidor de intercambiando los paquetes InATMARP iniciales.

El cliente maneja las actualizaciones de la tabla con el siguiente criterio:

- Cuando una entrada de la tabla degenera, el cliente la invalida.
- Si no hay un VC asociado a la entrada invalidada, se borra.
- En el caso de una entrada invalidada con un VC abierto, el cliente ATMARP revalida la entrada para ese VC antes de enviar cualquier información que no tenga nada que ver con la resolución de direcciones. Hay dos posibilidades:

- En el caso de un PVC, el cliente valida la entrada al transmitir un InARP_REQUEST y actualizar la entrada al recibir un InARP_REPLY.
- En el caso de un SVC, el cliente valida la entrada al transmitir un ARP_REQUEST al servidor ATMARP y actualizar la entrada al recibir un ARP_REPLY.

    - Si un VC asociado con una entrada invalidada de la tabla ATMARP se cierra, la entrada se elimina.

Como se menciona arriba, cualquier cliente IP de ATM que use SVC's debe conocer la dirección de su servidor ATM para el LIS concreto. Esta dirección se le debe indicar a cada cliente durante la configuración. Por el momento no hay ninguna dirección ATMARP bien conocida.

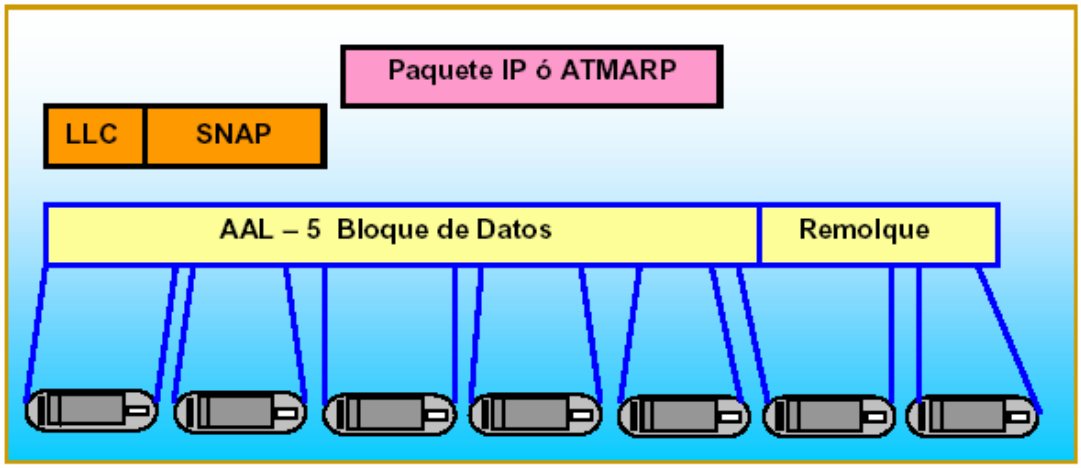
2.1.4 Formato de paquete

Hay dos métodos para el encapsulado de paquetes en los Protocolos de Internet IP clásicos sobre ATM. Cuando se transmiten paquetes IP y ATMARP sobre un simple canal virtual, el protocolo debe ser identificado por un campo de encabezado adicional en cada paquete. De forma alternativa se puede usar multiplexación de los canales virtuales VC con un canal virtual diferente para cada tipo de protocolo. Esta técnica se llama

también "encapsulación nula" Los paquetes son encapsulados usando IEEE 802.2 LLC/SNAP, como se describe en los documentos RFC 1483 [9] "Encapsulación de Multiprotocolo sobre la capa de adaptación ATM de nivel 5: AAL-5". Este método requiere de un encabezado de 8 bytes para cada paquete. El encabezado está compuesto por 3 bytes para el LLC (Logical Link Control ó Control de enlace lógico), que identifica que punto de conexión de la subred continúa. El campo SNAP (Sub-Network Attachment Point ó Punto de Conexión de Subred) está compuesto de 3 bytes para el Identificador Único Organización (OUI) y de 2 bytes para el Identificador del Protocolo (PID) definido por el OUI. El valor OUI: 00-00-00 indica que el PID está en una red tipo Ethernet, y el valor OUI 08-00 significa que el paquete siguiente es un IP; por ejemplo, el valor 08-06 marca que el siguiente paquete es un protocolo con capacidad de direccionamiento ARP.

La figura 6 muestra el encapsulado y la segmentación de un paquete IP a una secuencia de celdas ATM.

Fig. 6 Encapsulado y segmentación de un paquete IP a la secuencia de celdas ATM



2.1.5 Prueba del IP clásico sobre ATM

El Protocolo de Internet IP clásico sobre ATM es relativamente simple, pero las implementaciones deben ser probadas para asegurar una correcta operación e interoperabilidad entre los proveedores de los sistemas. Los procedimientos de encapsulado pueden verificarse simplemente decodificando las tramas capturadas en el enlace ATM. Los encabezados de control del enlace lógico y del punto de conexión de la subred (LLC/SNAP) deberían tener la forma: AA-AA-03-00-00-00-08-00 para los paquetes de Protocolos de Internet IP's. La codificación correcta de los paquetes ATMARP es un poco más complicada, ya que el formato del paquete es una modificación del protocolo tradicional ARP. Un punto de interpretación diferente está en como se codifican las direcciones

desconocidas. Los paquetes ATMARP tienen una longitud de campo para cada dirección de las estaciones A y B. Una petición de mensaje podría codificar el campo de la dirección desconocida del cliente B en una de las dos formas siguientes:

1. Longitud cero y ausencia del campo de dirección.

2. Longitud correcta (por ejemplo 4 bytes para las direcciones IP, y 20 bytes para las direcciones ATM) y, una dirección cero (ejemplo: 0.0.0.0) para IP.

Este tema surgió en las sesiones de pruebas de interoperabilidad de multimarcas conducidas en la Universidad de New Hampshire en Febrero de 1995, y se consulta en el pedido de comentarios de los estándares de Internet RFC 1577. Las diferentes discusiones entre varios fabricantes concluyen que los mensajes deberían estar codificados usando el último método, pero que los mensajes recibidos puedan usar cualquier codificación que sea interpretada correctamente. Luego de esto, será propuesta una actualización de la RFC 1577, de modo que la longitud del campo de direcciones pueda ser interpretada como el número de bytes de dirección a proponerse, en un buffer de longitud fija de 20 ó de 4 bytes. Esto tiene una consecuencia muy significativa en la interoperabilidad ya que las implementaciones de la longitud del campo de direcciones, no la longitud de la dirección determinará el tamaño del buffer o de la memoria temporal requerida.

Otra característica de interoperabilidad que se debe considerar es cómo codificar la respuesta del protocolo con capacidad de dirección, para manejar el reconocimiento negativo ARP-NAK (negative AcKnowledgement). Este mensaje es una nueva extensión para el NTMARP, que indica que la dirección requerida no se puede encontrar. En los protocolos ARP tradicionales, la estación que pregunta esperaría por una respuesta del ARP de la dirección de destino durante un tiempo (time out) antes de considerar como un error la falta de respuesta.

El RFC 1577 establece que el servidor simplemente devuelve una copia del mensaje de pedido, pero con el código de operación cambiando de 1 (pedido de ARP) a 10 (No Reconocimiento de ARP).

Este procedimiento es contrario a una respuesta normal, donde los campos de las direcciones de A y B son cambiadas. Deben escogerse algunas implementaciones para codificar un mensaje de respuesta con direcciones cambiadas, e insertar bien el código de operación para leer exitosamente la dirección. Puede haber problemas en las implementaciones que verifiquen los campos del mensaje ATMARP según el intento inicial del RFC 1577. Las pruebas de funcionamiento del protocolo de un cliente ó del servidor pueden ser optimizadas utilizando un probador de protocolos para simular un extremo de la conexión. Por ejemplo, el probador puede iniciar la conexión hacia el servidor y responder al pedido inicial de InARP, ó enviar un pedido de ARP usando direcciones diferentes de IP, conocidas o

desconocidas. Las respuestas (ARP ó ARPNAK) deberían corresponder a la tabla de direcciones del servidor, que pueden ser examinadas por un terminal conectado al dispositivo.

2.1.6 Resultados de desempeño

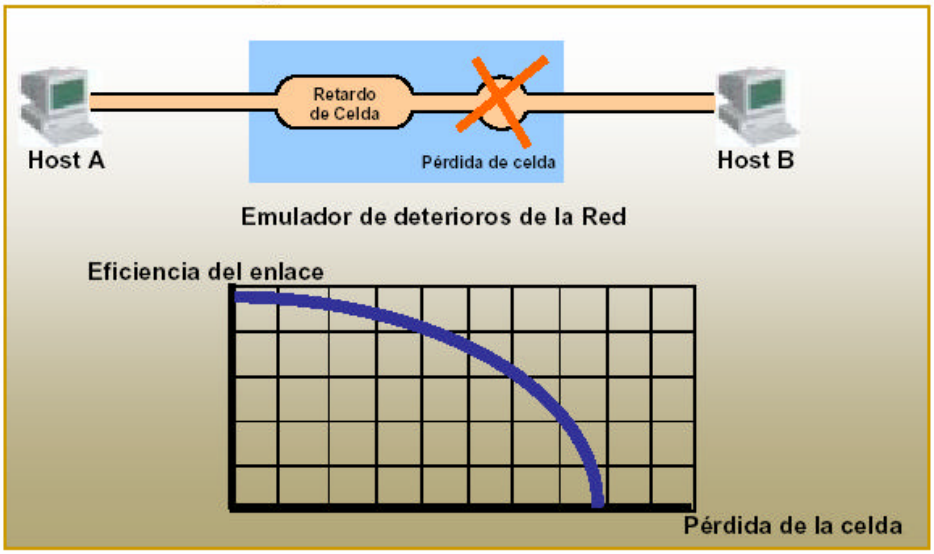
Una consideración importante para las implementaciones de la RFC 1577 es la aplicación final del desempeño. El desempeño es un término relativo, y depende de muchos factores, entre ellos la tasa de transmisión (con o sin congestión), de las implementaciones del protocolo y de la arquitectura del sistema. El desempeño del protocolo del control de transmisión TCP depende del llamado "Producto de Ancho de Banda - Retardo". Simplemente indica el ancho de banda multiplicado por el tiempo de retardo en la transmisión de los datos a través del enlace completo. Por ejemplo, la capacidad de un proceso de comunicaciones de un TCP (Pipe) para un canal virtual de 10 Mb/s con un retardo total de 15 ms es de 18.750 bytes. El tamaño de la ventana del TCP corresponde al total de los datos no reconocidos que pueden ser manejados correctamente, y deberían ser el menos de ese tamaño para lograr un máximo resultado en la transmisión de los datos comunicados. El retardo total puede ser medido sobre una conexión por medio del programa conocido como "ping". Esta herramienta de redes envía paquetes de Eco (ICMP ó Internet Control Message

Protocol) a la dirección. IP de destino y examina la respuesta del paquete Eco desde esa dirección una marca de tiempo de salida, con una precisión de 1 microsegundo, se inserta en el paquete de Eco y se resta del tiempo de la respuesta del Eco recibido para calcular el tiempo de retardo total. Esta técnica toma en cuenta el tiempo procesamiento del software a cada extremo. Estas pruebas, llamadas pruebas “ping", podrían ser usadas para medir a groso modo el tiempo de conexión del Setup. El ping inicial puede ser significativamente más largo que los pings remanentes en un ambiente de canal virtual conmutado SVC, ya que la dirección ATM puede requerir ser obtenida desde el servidor de ATMARP, y el canal virtual debe estar establecido. En este caso, una medición del retardo en la conexión del setup debe hacerse con un probador de protocolo monitoreando la línea, como el HPJ2302B: AN LAN E1/ATM Internet Advisor.

TPC sobre redes de alto desempeño: regresando al tema el producto entre el ancho de banda y el retardo podemos observar que cuando el ancho de banda se incrementa, el tamaño de la ventana debe incrementarse para asegurar una máxima calidad de transmisión. El tamaño de la ventana del TPC se forza de un campo de 16 bits a uno de 65.536 bytes. Por lo tanto, la calidad del enlace también se limita, a menos que el tiempo de retardo se reduzca.

Si podemos usar una ventana de tamaño grande para el TCP, lo que significa que podemos tener más datos desconocidos en el proceso de comunicaciones (pipe), y si un paquete se pierde, el TCP borrará normalmente los paquetes desconocidos como parte de su proceso de recuperación. Con una ventana grande, puede lograrse una calidad aceptable en la transmisión. En una red de ATM, la pérdida de una simple celda ocasionaría la pérdida de un paquete en la capa de adaptación ATM (AAL-5); y, el efecto aumentaría el tamaño del protocolo. Una herramienta para medir el desempeño del protocolo de control de transmisión TCP es el "tcp", que opera como una fuente de tráfico de TCP en una estación UNIX y actúa como un host ó dispositivo inteligente conectado a la red y mide la eficiencia del enlace que una aplicación podría experimentar. Los diseñadores de redes deberían permitir un ajuste fino de los parámetros configurables del TPC para optimizar la eficiencia del enlace. Un diseñador puede también necesitar la medida de la calidad del enlace, para la aplicación, cuando los errores se introducen en el nivel de ATM.

Fig. 7 Emulación de detectores de celda



Algunos experimentos han mostrado que hay un punto en el cual los deterioros de la red causan que el desempeño del TCP caiga dramáticamente. La correlación inicial, entre la pérdida de la celda y la eficiencia en la transmisión del paquete alcanza un valor luego del cual la aplicación llega a ser virtualmente inusable, a pesar de que un significado monto de los datos de la celda sean recibidos correctamente.

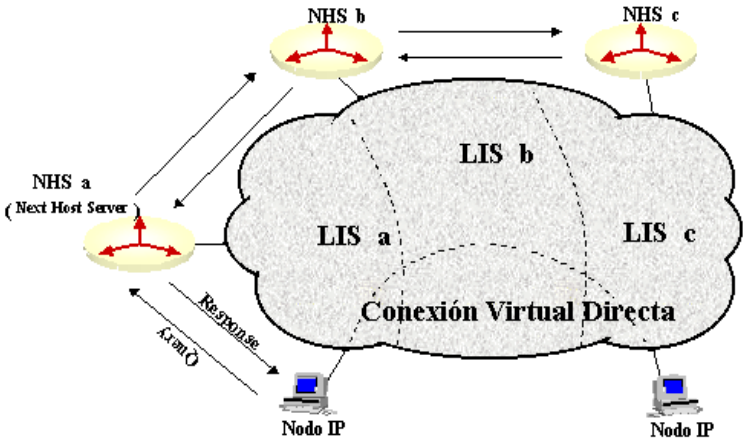
2.1.7 Comunicación fuera de la subred LIS

La RFC 1577 no aborda el tema de que dos dispositivos que se encuentren en distinta LIS puedan establecer un circuito virtual para comunicarse.

Los equipos de distintas *LIS* son interconectados a través de los routers, lo cuales son los encargados de desencapsular el paquete *IP* de la capa *AAL5*.

Para evitar las pérdidas por latencia en la comunicación entre *LIS* lejanas, se utiliza el protocolo *NHRP* [10] (*Next Hop Resolution Protocol*). Cada *LIS* tiene un *NHRP Server* (*NHS*), y cada elemento final un cliente *NHRP*. El *NHS* resuelve los pares de direcciones *IP-ATM*, con la diferencia, respecto a los servidores *ATMARP*, que cada *NHS* realiza una conexión directa con el *NHS* más cercano al nodo destino sin necesidad de atravesar los routers intermedios. Esto requiere un proceso de *broadcasting* que actualice cada uno de las tablas de ruta de los *NHS*.

Fig. 8 Comunicación fuera de la subred LIS



Tanto *Classical IP-ATM* como *NHRP* solamente soportan conexiones *unicast*. Para realizar conexiones *multicast* es necesario traducir las direcciones *IP multicast* a listas de direcciones *ATM*, acción que realiza un "*Multicast Address Resolution Server"* (*MARS*), y determinar cómo se transferirán los datos, ya sea mediante una malla de *VC's* todos con todos o mediante un "*Multicast Server*" (implica una latencia adicional).
Los *MARS* resuelven las peticiones igual que un *ATMARP*, para lo cual los elementos finales mandan paquetes.

La arquitectura MPOA, Multiprotocol Over ATM [11] (Multiprotocolo a través de ATM), del ATM Forum, contempla la integración de IP con ATM mediante emulación de LAN versión 2 y NHRP.

2.1.8 Ventajas e inconvenientes del IP clásico

El IP clásico sobre ATM es una solución eficiente para aplicaciones de paquetes de datos en un Área local, pero no soporta redes WAN eficientemente. Los paquetes destinados a direcciones que están fuera de la subred lógica LIS deben ser enrutados, requiriendo un encabezado extra y añadiendo un retardo con cada enrutador. Esta deficiencia está siendo

tratada dentro del IP, sobre el Grupo de trabajo de ATM, en donde el siguiente protocolo de enrutamiento conocido como NHRP (Next Hop Routing Protocol) ha sido propuesto para reemplazar el ATMARP. Los pedidos de dirección que no han sido resueltos en la subred lógica local LIS pasan a servidores adicionales en otras subredes LIS. Entonces, la dirección ATM de destino retorna y se crea un canal virtual a través de la red. Este enfoque resuelve el problema de retardo, pero puede originar un retardo significativo en el setup o disposición del sistema. Algunos fabricantes están tratando las limitaciones del TCP en redes de alta velocidad con nuevas opciones, descritas en el RFC 1323 [12] "Extensiones de TCP para Alto Desempeño". Además, usan algunos algoritmos para retransmisión y recuperación más rápidas, que alivian los efectos de las pérdidas de paquetes con ventanas grandes.

Capítulo 3

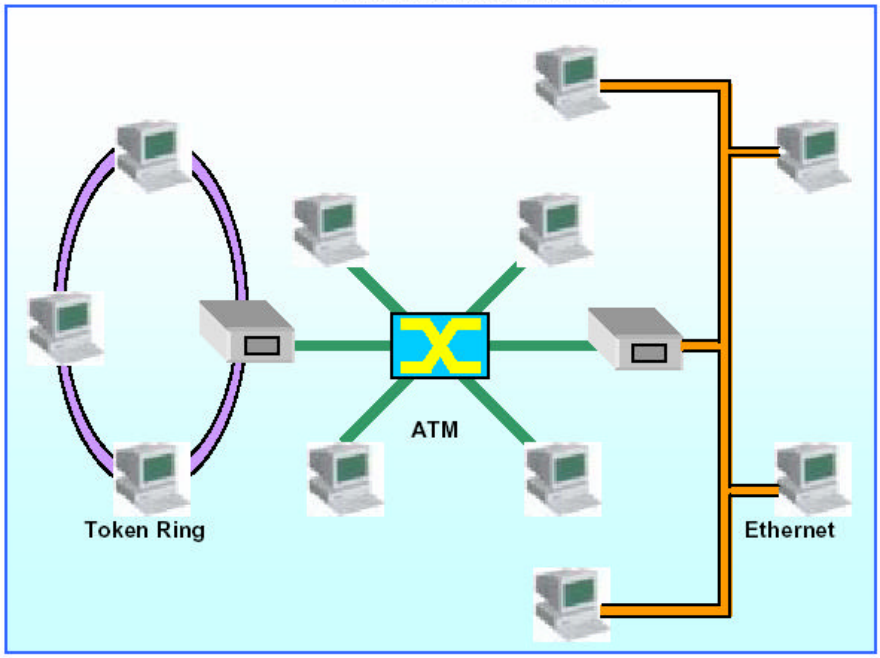
3.1 Emulación de LAN

Mientras que el IP clásico sobre ATM es usado para traer el ATM a las redes de Área local, no permite direccionar bien el conjunto de tecnologías LAN existente. Se necesitan paquetes para ser enrutados entre los diferentes tipos de redes, siendo el IP el único protocolo soportado.

El Foro de ATM reconoció que la interoperabilidad con las redes LAN y las aplicaciones existentes es muy importante para la aceptación de ATM en el mercado. El subgrupo de trabajo para Emulación de LAN's definió inicialmente un servicio que emula las características de las redes LAN existentes. Esta emulación tiene lugar en la capa del MAC[13] (Media Access Control), de modo que la red ATM mire efectivamente como a una red LAN tradicional a la aplicación determinada. Un amplio rango de protocolos (tales como el NETBIOS, el IPX y el Appletalk) operaran sobre esta interfase. El resultado final es que una simple red de Área local puede ser compuesta de segmentos ATM y de segmentos con varias topologías LAN. Al momento, pueden ser emuladas las tecnologías Ethernet y Token-Ring.

La figura 9 muestra una pequeña red con dos LAN's emuladas (ELAN's).

Fig. 9 Emulación de redes LAN



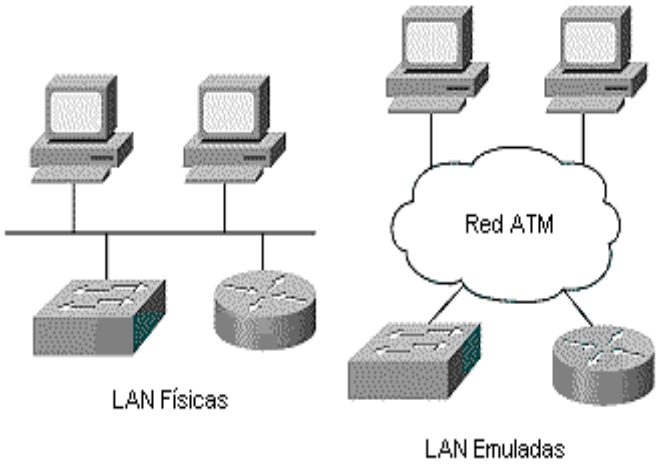
La mayor diferencia entre las redes LAN's y las redes ATM es que las ATM son orientadas a conexión, mientras que las LAN usan un medio comparativo para conectar sus terminales. Los protocolos LAN envían paquetes de datos a todas las estaciones de la red, para que sean recibidos por los destinatarios direccionados y sean ignorados por las demás estaciones.

Una emulación de ATM de este funcionamiento requiere la habilidad de emitir paquetes hacia múltiples destinos.

Como el nombre lo sugiere, el protocolo LANE es emular una red LAN (Local área Network) sobre una red ATM. Específicamente el protocolo LANE define

mecanismos para emular tanto una red Ethernet como una Token Ring. La emulación LAN, significa que los protocolos LANE definen una interfaz de servicios para los protocolos de las capas altas (capa de red), la cual es idéntica a las de las LAN's existentes, y la data enviada a través de la red ATM es encapsulada en el formato de paquete apropiado. En otras palabras, los protocolos LANE hacen que la red ATM, se vea y se comporte como una red Ethernet o Token Ring [14]; aunque operando mucho más rápidas que una de ellas.

Fig. 10 Emulación de redes LAN



Como ya se había mencionado la forma más flexible para integrar las estructuras existentes de LAN's tradicionales a redes ATM es la emulación completa de capa LAN—MAC. De esta manera, todas las aplicaciones LAN existentes pueden ser usadas vía redes ATM sin ninguna modificación.

3.1.1 Arquitectura de Emulación de LAN

Hay varios componentes en la arquitectura de Emulación de LANS. Algunos clientes de emulación de LAN's (LEC's ó Lan Emulation Clients) se comunican con un servicio de emulación de LAN's a través de un interfase de red para usuario de emulación LAN (LUNI ó Lan Emulation User to Network interfase). Cada estación terminal ATM es asociada con un LEC ó cliente de emulación de LAN. Esta asociación incluye la interfase ATM con el puente hacia la red LAN.

El LEC es responsable de proveer la emulación de la capa MAC para niveles mayores de protocolo.

El servicio de emulación de LAN's por si mismo tiene 3 componentes:

1. El servidor de Emulación de LAN's (LES ó Lan Emulation Server): responsable de la resolución de la dirección desde los MAC's hasta las direcciones de los ATM.

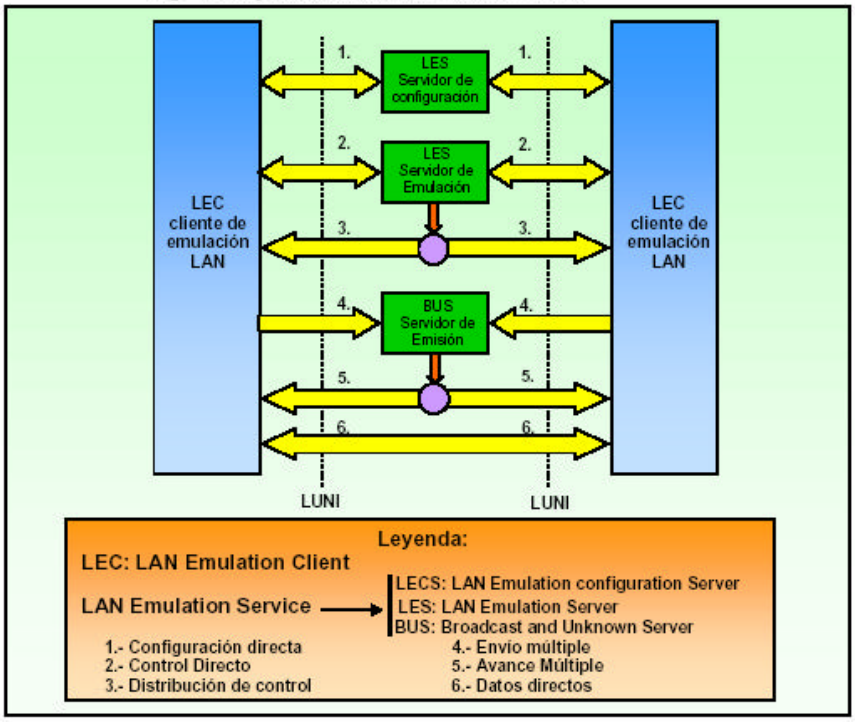
2. Servidor de Emisión y de Dirección Desconocida (BUS ó Broadcast and Unknown Server): El BUS es un servidor multiemisor (Multicast) que es utilizado para fluir el tráfico de las direcciones destino desconocidas y reenviar el tráfico de los emisores y multiemisores a los clientes en una

ELAN en particular. Cada Lec es asociado con un solo BUS por ELAN, pero hay puede haber muchos BUS's dentro de una ELAN que comunique y coordine de manera específica. La conexión del BUS al LEC es identificado por una dirección ATM, en el LES, ésta es asociada con el emisor de direcciones MAC y este mapeo es configurado normalmente hacia el LES.

3. Servidor de Configuración para Emulación de LAN's (LECS ó Lan Emulation Configuration Server): Usado por los clientes para su configuración inicial.

La arquitectura del sistema permite a estos componentes estar distribuidos entre varios dispositivos físicos. Estos tres componentes se comunican entre ellos a través de varios canales en los interfaces de red para usuarios. Algunos de estos canales virtuales son unidireccionales, otros pueden ser implementados como punto a multipunto. La figura 11 muestra las conexiones entre los componentes de emulación de LAN's:

Fig. 11 Arquitectura de la emulación LAN



Formato de Paquete: los paquetes de Emulación de LAN's son codificados usando un formato nuevo de trama. El Foro de ATM escogió no usar el método de encapsulado LLC/SNAP [15] (Logic Link Control/ SubNetwork Attachment Point) para las tramas IEEE 802.3 de Ethernet ó IEEE 802.5 de Token Ring, conforme a lo descrito en el RFC 1483. En lugar de estos arreglos de entramado, el formato de paquete se definió de modo que compartan un encabezado común inicial entre los paquetes de control y de datos.

Los paquetes de datos empiezan con un campo de 16 bits que identifican al cliente LEC envía los datos. Este valor debe ser menor que OxFF00, ya que

se usa para identificar los paquetes de control. Los paquetes de datos de Ethernet tienen un encabezado diferente que para los de Token Ring.

El Token Ring es un protocolo fuente enrutado, que permite también enrutar la información contenida en el encabezado del paquete. Adicionalmente, el ordenamiento de los 48 bits de la dirección del MAC (Media Access Control) es diferente, ya que el Ethernet transmite primero el bit menos significativo y el Token Ring el más significativo.

3.1.2 Operación de la Emulación de LAN's

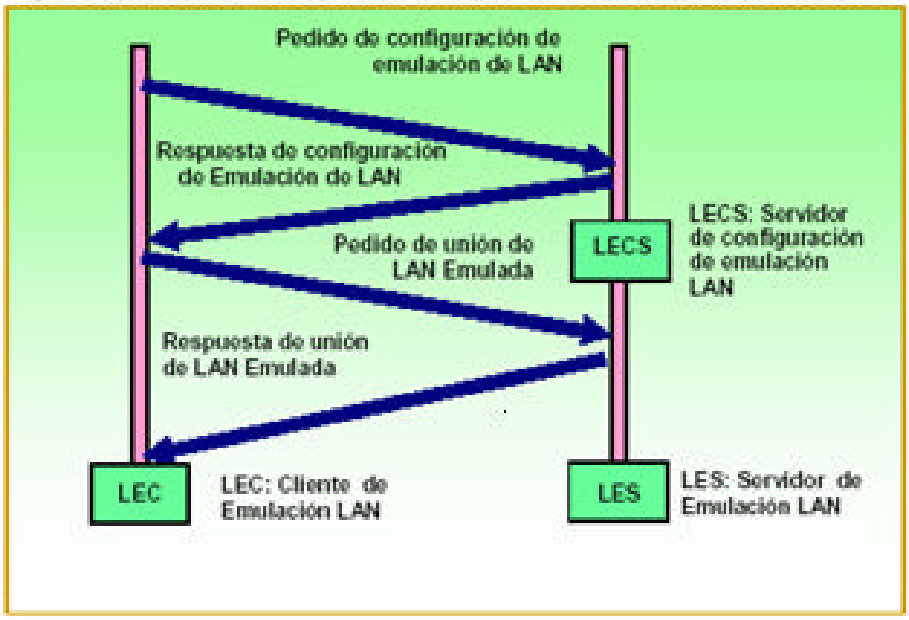
Los protocolos de Emulación de LAN's son complejos de modo que se resumirán a continuación sus pasos de operación:

1. **Inicialización del Cliente:** El cliente LEC debe ser inicializado antes de que pueda enviar los datos a otros LEC's. La inicialización empieza cuando el LEC hace una conexión al servidor de configuración LECS. Primero trata de conseguir la dirección ATM para el servidor LECS con un pedido de interfase provisional de manejo local (ILMI ó Interim Local Management interfase). Si éste falla, se usara una dirección bien conocida de ATM. El cliente LEC entonces intenta arreglar un canal virtual conmutado SVC bidireccional para esta dirección. Si otra vez falla, el cliente LEC usará un canal virtual permanente PVC [16] como último recurso. Una vez que ha sido establecida esta conexión de Configuración Directa, el cliente LEC

envía su dirección ATM en un mensaje de pedido de configuración al servidor LECS. Este servidor de configuración contesta con la dirección del servidor de Emulación de LAN's ó LES y con el nombre y tipo de red LAN emulada (Ethernet o Token Ring). Algunos parámetros adicionales de configuración (como valores de contador o de tiempo) pueden también formar el mensaje de respuesta del servidor de configuración de las redes de LAN emuladas.

El siguiente paso del cliente LEC es establecer la conexión de Control Directo con el servidor LES. Este canal virtual conmutado SVC es usado para enviar un pedido del cliente LEC para unir la red LAN emulada. Si la conexión es exitosa el servidor LES retornará un identificador único del LEC (LECID) que será incluido en el control futuro y en el envío de los paquetes de datos por parte del cliente. El servidor LES tiene la opción de responder al cliente en la conexión de Control Directo, ó a través de una conexión de Control Distribuido punto multipunto unidireccional a todos los clientes LEC's servidos por LES. La figura 12 muestra los pasos de inicialización para unir un cliente LEC en una red LAN emulada (ELAN).

Fig. 12 Pasos de la inicialización de la unión de cliente LEC con la red



2. Registro y Resolución de la Dirección: cada cliente LEC debe registrar la dirección (ó direcciones) del control de acceso al medio MAC que representa, en el servidor LES. Este servidor construye una tabla de direcciones de ATM (pares de direcciones de MAC's que usa para responder a los pedidos de resolución de dirección que hará el cliente LEC luego). Este protocolo es similar al ARP (Address Resolution Protocol) que se usa en las arquitecturas clásicas de IP sobre ATM, como se vio en la primera parte de este artículo. Una diferencia clave está en que si el servidor no puede responder al pedido, sí puede decidir el envío del pedido al cliente registrado en esa MAC, ó puede enviar el pedido a todos los

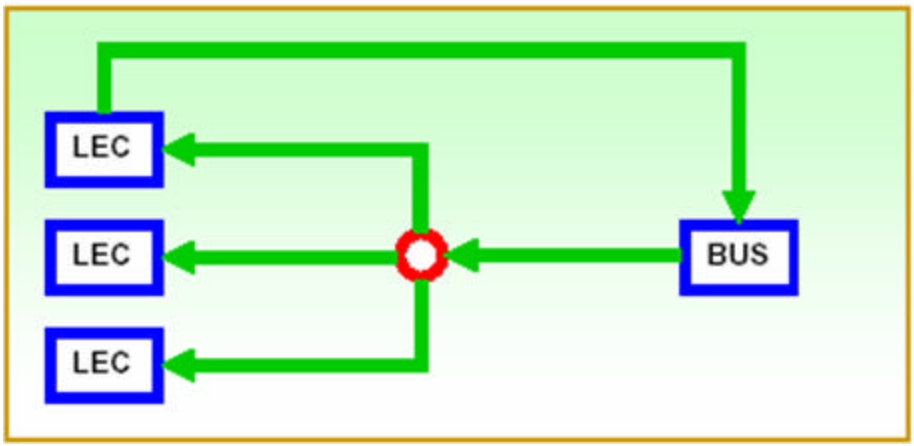
clientes a través de la conexión punto - multipunto de Control Distribuido. El cliente que representa la dirección del MAC responderá al cliente que pregunta, enviándole la dirección ATM correspondiente.

3. Transferencia de Datos: es este punto, un canal virtual conmutado SVC [17] de Datos Directos puede ser inicializado entre dos clientes. El encabezado de emulación de la LAN es reclamado por la trama de control de acceso al medio, y el paquete de datos se envía de cliente a cliente. Normalmente, cada conexión de Datos Directos termina. Si no se envían paquetes entre los clientes por más de 20 minutos, el canal virtual conmutado se desconecta. Una conexión nueva puede ser establecida entre estos clientes si es necesaria más tarde. Hay otra alternativa para enviar datos a un cliente. El servidor de emisión y de dirección desconocida (BUS) puede ser usado para enviar datos a una dirección x antes de recibir una respuesta. Cada cliente debe establecer una conexión de envío de multiemisión (Multicast Send) hacia el servidor de emisión BUS, que pone al cliente en una conexión unidireccional punto –multipunto (Multicast Forward) para los datos de retorno. El cliente obtiene la dirección de ATM del BUS enviando un pedido ARP al servidor, usando la dirección del MAC de emisión (todos "unos").

Cuando el cliente envía un paquete al servidor de emisión BUS, este lo distribuye a todos los clientes LECS. La dirección de destino en el paquete

de datos determina cuál LEC lo procesará La figura 13 ilustra la operación del servidor de emisión de dirección desconocida (BUS).

Fig. 13 Operación del servidor de emisión de dirección desconocida de BUS



4. Dificultades de implementación: la emulación de las redes LAN es un tema candente para muchos fabricantes, pero esto conlleva un complejo juego de protocolos. En consecuencia, esta ligada a una implementación difícil. Se han estimado que el software de los servidores de emulación de LAN's toma cerca de 50.000 líneas de códigos en C, y que la implementación de los clientes es del orden de las 20.000 líneas. Como se puede apreciar, la corrección de estos componentes es una tarea muy admirable y digna de los pacientes diseñadores de software.

Hay algunos puntos posibles de falla en el proceso del protocolo. Hay que tener cuidado para asegurar que el cliente y el servidor permanezcan sincronizados, aún cuando otros sistemas fallen (como la señalización).

Podría haber problemas imprevistos, tales como condiciones diferentes entre los pesos del proceso de configuración.

5. Desafíos de las pruebas: los componentes de prueba de la emulación de redes LAN pueden ser caracterizados en diferentes niveles. Las pruebas de la capa física y de ATM pueden ser hechas en un dispositivo como un puente. Por ejemplo, el tiempo de espera para el acceso a la red a través del puente, puede ser medido capturando una marca de tiempo en el paquete Ethernet en un lado del puente, y correlacionándolo con la marca de tiempo del paquete capturado en el lado ATM. Se requiere una base de tiempo común entre los dos interfaces físicos.

La interoperabilidad entre los protocolos es un tema para la emulación de LAN's, ya que muchos fabricantes producen equipos para clientes y servidores. Los fabricantes de los clientes de redes LAN emuladas demandan muchas implementaciones en los servidores. Las pruebas de interoperabilidad y de compatibilidad serán definidas por la Emulación de las redes LAN. Por ahora, los grupos de pruebas de calidad desarrollados, observan manualmente las comunicaciones cliente - servidor para concordar con las especificaciones.

3.1.3 Redundancia de LANE

Introducción

La versión 1.0 de LANE define los estándares para la comunicación entre redes de área local tradicionales como Ethernet y Token Ring con equipos conectados a ATM. Este tipo de equipos incluyen estaciones finales y servidores, conmutadores LAN-ATM y routers conectados a ATM para encaminar tráfico entre ELAN's.

Sin embargo, como la versión 1.0 de LANE no define mecanismos de redundancia en los servicios LANE, los servidores LANE se convierten en puntos únicos de fallo. Además, también se necesitan resolver los temas de redundancia del router y de los caminos/enlaces. Cisco ha desarrollado varios mecanismos que pueden ser utilizados para construir redes ATM tolerantes a fallos:

- Simple Server Replication Protocol (SSRP) para la redundancia de servicios LANE, que funciona con LEC's de Cisco y igualmente que de cualquier tercero.
- Hot Stand by Router Protocol (HSRP) sobre LANE, que proporciona redundancia para el router de defecto configurado en estaciones finales IP.

- Tarjeta LANE de PHY doble en el Catalyst 5000 o múltiples enlaces en el Catalyst 3000.
- Protocolo Spanning Tree en conmutadores ATM de Ethernet.

El problema principal de LANE 1.0 es que un cliente o LEC solo puede acceder a un grupo de servidores LANE:

- Un solo LECS soporta todos las ELAN's en un dominio ATM
- Solo puede haber un par LES/BUS por cada ELAN

Un fallo en cualquiera de estos componentes afecta al funcionamiento de la red. Más específicamente:

- Fallo del LECS: Un fallo del LECS tiene un impacto sobre todas las ELAN's al proporcionar control de acceso para todas ellas. Aunque las ELAN’s existentes siguen funcionando normalmente (se asumen solo LEC’s de Cisco), ningún nuevo LEC se puede unir a cualquier ELAN bajo el control de ese LECS.

- Fallo de LES/BUS: El par de LES/BUS se necesita para mantener un ELAN operacional. El LES proporciona el servicio LE_ARP para la asignación de direcciones ATM/MAC y el BUS proporciona broadcast y búsqueda de direcciones desconocidas para una ELAN. Por eso, un

fallo en el LES o el BUS tiene un impacto inmediato sobre la comunicación en la ELAN.

Redundancia en Redes LANE 1.0

El protocolo de redundancia LANE, SSRP consiste principalmente en reforzar los componentes de servicios LANE: LECS, LES y BUS. Para la redundancia de LECS, un LECS primario es apoyado por varios LEC's secundarios. La redundancia de LES/BUS se maneja de una forma similar, donde un LES/BUS primario es apoyado por varios secundarios.

Simple Server Redundancia Protocol (SSRP), se ha desarrollado para proporcionar servicios LANE redundantes. Aunque muchos vendedores han incorporado servicios LANE redundantes de algún tipo, todos estos servicios no cumplen con la especificación LANE 1.0 por lo cual no son interoperables con implementaciones de terceros. Sin embargo, SSRP si cumple la especificación LANE 1.0 y es interoperable con clientes LANE de terceros fabricantes, una consideración muy importante cuando se quiere implantar una red interoperable ATM.

Se debería tomar nota de que la discusión sobre la redundancia de LANE en este documento habla de fallos en mecanismos de servicio LANE

(LECS/LES/BUS) y no se consideran las necesidades de redundancia a nivel de backbone ATM. La redundancia en el backbone ATM se resuelve, mediante la utilización de protocolos como PNNI pero no entraremos en detalles al respecto.

3.1.4 Ventajas y Desventajas

Ventajas:

- **Facilidad de administración**

  Las funciones de administración se centralizan en el LECS de forma que el administrador puede definir diversas ELAN's en la red ATM y asignarlas a puertos de los conmutadores, routers o host ATM independientemente de su ubicación física. Aquellos puertos o host que precisen pertenecer a más de una ELAN podrán hacerlo siempre que sus tarjetas ATM soporten más de un LEC.

- **Facilidad de movimientos y cambios**

  La pertenencia a una ELAN se mantiene aunque se produzcan movimientos y los cambios de ELAN no suponen ningún cambio físico.

- **Multiprotocolo**

  LANE es esencialmente un protoloco de nivel 2 sobre ATM y por tanto, totalmente independiente de los protocolos de nivel superior.

Desventajas:

- **Aplicable solo a Ethernet y Token Ring**

  LANE define métodos de emulación para Ethernet y Token Ring únicamente. La existencia de tráfico FDDI implica la utilización de técnicas de Translational Bridging de forma que dicho tráfico es convertido a tráfico Ethernet o Token Ring.

  No explota las funcionalidades ATM de QoS (Quality of Services) o calidades de servicio LANE, por definición, oculta las características de ATM a los protocolos de nivel superior y una de las características esenciales de ATM es QoS. Las únicas clases de servicio soportadas por LANE son UBR (Unspecified Bit Rate) y ABR (Available Bit Rate) por ser estas las más cercanas a la naturaleza de los protocolos a nivel MAC. Este inconveniente no es tal comparado con otras técnicas de definición de

VLAN's dado que el concepto de QoS no se considera en el resto de las definiciones.

- **Problemas de control de broadcast**

LANE, al igual que cualquier protocolo de nivel 2 es susceptible de sufrir tormentas de broadcast por lo que debe limitarse la definición de ELAN a pequeños grupos de usuarios. Esto implica que redes grandes existirá un gran número de ELAN’s por lo que el rendimiento de los servidores LANE (especialmente del servidor BUS) es esencial.

Capítulo 4

4.1 Multiprotocolo Sobre ATM (MPOA)

4.1.1 Introducción

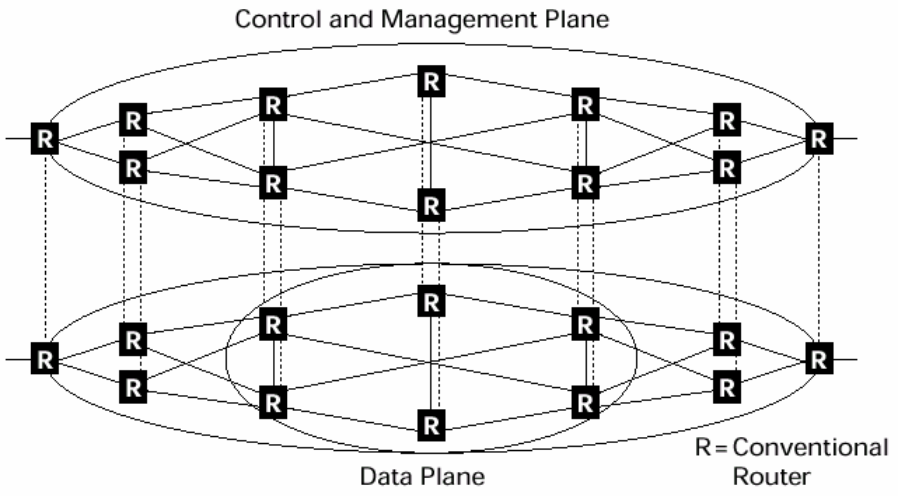
El reto fundamental para una red basada en enrutadores llega cuando el crecimiento de las redes en tamaño y nuevas aplicaciones hace uso de grande cantidades de datos, así como tráfico multimedia sensible a los retardos. Como uno de los primeros pasos para responder a las quejas de los usuarios por el bajo desempeño, el administrador de la red intenta remediar el ancho de banda en el escritorio mediante el uso de switches LAN de alta velocidad en los bordes de la red y switches ATM para sus backbones. Como los usuarios continúan enviando y recibiendo grandes cantidades de tráfico a través de los límites de la subred, la misma LAN y los switches ATM ahora envían millones de paquetes por segundo a sus enrutadores de backbone. Aún los routers más rápidos, capaces de procesar hasta 500,000 paquetes por segundo, se convierten en cuellos de botella para el tráfico de la subred generado por el uso penetrante de Internet, intranets y el tráfico multimedia.

Los enrutadores también introducen retardos dado que ellos desarrollan las tareas de resolver direcciones, determinar enrutamientos y filtrar paquetes. Mientras mayor sea el tráfico y más saltos de enrutamiento el tráfico

encuentre para alcanzar su destino final, mayor será el retardo causado por los enrutadores. Para hacer esto peor, la latencia de cada trama varía, resultando en una variación del retardo, la cual no es determinística por naturaleza e inapropiado para aplicaciones multimedia.

Los enrutadores usualmente aceptan tramas de la capa de red direccionadas a ellos desde hosts conectados a las subredes LAN y las reenvían a los hosts de destino en otras subredes. Esto opera en un modo sin conexión, de acuerdo al protocolo de enrutamiento que esta siendo usado.

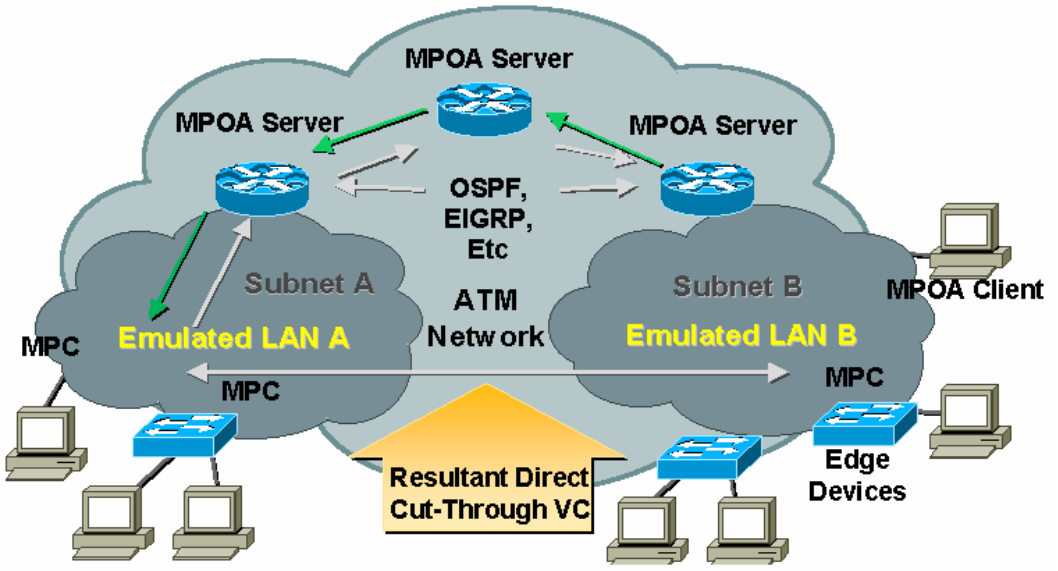
Fig. 14 Direccionamiento y mapeo dentro del enrutador



Como se muestra en la Figura 14, en un medio sin conexión, cada trama dentro de un flujo de datos está sujeta al procesamiento en el mapeo de direcciones dentro de un enrutador y este proceso es repetido para cada salto de enrutamiento en la red. Esto implica que cada enrutador en la red arriba mostrado debe correr o ejecutar el stack de enrutamiento multiprotocolo. Esto no solo es costoso desde la perspectiva del software y el equipo, sino que también complejo desde el punto de vista de la gestión de una red. Cada enrutador en la red debe ser configurado independientemente, mantenido y administrado.

En algunos casos, para mejorar el desempeño, los enrutadores pueden simplemente ser reemplazados por switches ATM de alta velocidad, pero haciéndolo así, todas las tareas efectuadas por los enrutadores se pierden. De modo del reto es integrar la funcionalidad de enrutamiento con la infraestructura de ATM sin imponer cuellos de botella o latencias significativas en el tráfico. Este reto se amplia cuando los requerimientos incluyen grandes poblaciones, sobre grandes áreas, con cargas de tráfico pesado y mezclado. También es claro que la solución resultante debe integrar las ventajes de la tecnología ATM con las tecnologías LAN como Ethernet y Token Ring para preservar la inversión en el hardware existente, y con TCP/IP e IPX/SPX para preservar la compatibilidad con la base de aplicaciones masivamente instaladas.

Fig. 15 Diagrama completo de MPOA



El Forum ATM ha aprobado un nuevo estándar conocido como Multiprotocol over ATM (MPOA), que proporciona la posibilidad de conmutar tráfico inter-VLAN sobre el backbone ATM de forma que solo el primer paquete de un flujo atraviesa el router y el resto se conmuta sin pasar por el router. Esta técnica, conocida como routing cut-through inter-VLAN, proporciona un rendimiento mucho más alto que routing tradicional, y es la tecnología apropiada a utilizar por servidores de Web, y otros servicios a los que acceden grandes grupos de usuarios.

En otras palabras se trata de una solución de routing para la capa de red que integra los protocolos existentes y los estándares para dar funciones de

routing sobre las redes ATM. Confiere escalabilidad y flexibilidad introduciendo un concepto conocido como ***routing virtual*** [18]. Este emula la funcionalidad de los routers tradicionales y elimina las limitaciones en el rendimiento que tiene el router salto a salto.

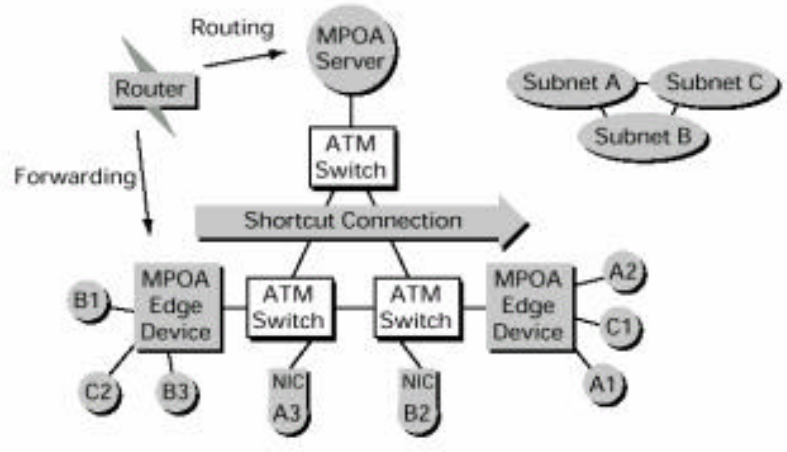
Para ello se establecerán atajos sobre el conmutador ATM entre cualquier host o dispositivo en los extremos con capacidades MPOA, independientemente de la subred a la que pertenezca. En resumen MPOA identifica flujos datos y los mapea directamente en canales virtuales ATM: MPOA emplea tres técnicas complementarias: LANE, NHRP y el concepto de router virtual.

4.1.2 Multiprocolo sobre ATM

El foro de ATM ha trabajado en cooperación con la IETF para desarrollar el MPOA— una poderosa solución de enrutamiento de la capa de red que integra y fortalece los protocolos y estándares existentes para proveer la funcionalidad de enrutamiento sobre redes conmutadas de ATM. Provee una escalabilidad y flexibilidad sin precedentes introduciendo un concepto conocido como “enrutador virtual”. El “enrutador virtual” emula la funcionalidad de las redes enrutadas tradicionales, pero elimina las limitaciones de desempeño del enrutamiento por saltos. Conexiones

abreviadas o “shortcuts” son establecidas sobre la fábrica de ATM desde cualquier host o dispositivo de borde que soporte MPOA hacia cualquier otro, sin importar la subred a la que pertenezca. En esencia, el MPOA identifica el “flujo” de datos y los mapea directamente a los canales virtuales de ATM. Esta técnica de establecimiento de “shortcuts” directamente a través de las redes ATM es a veces referido como “cutthrough” o enrutamiento “zero-hop”.

Fig. 16 Establecimiento de una conexion

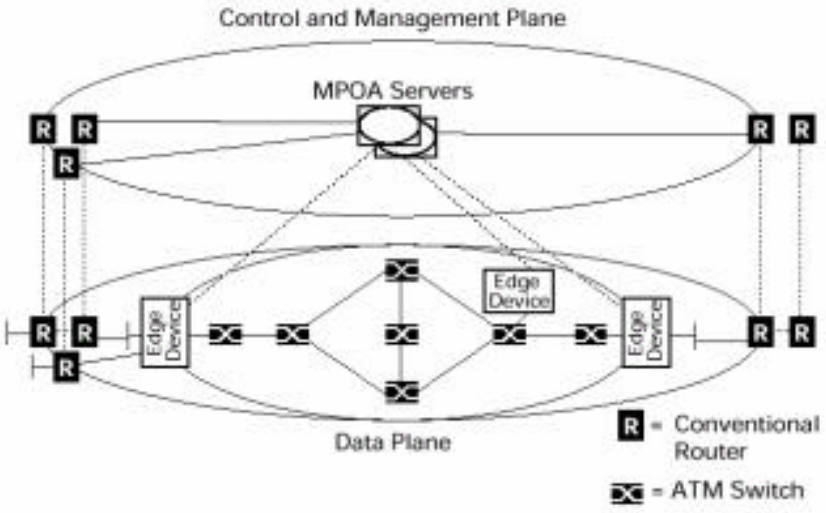


El establecimiento de una conexión “shortcut” sobre ATM ofrece una significativa mejora en el desempeño comparada con una solución basada en enrutamiento puro. Los paquetes transportados cobre una conexión abreviada no son sujetos a un enrutamiento por saltos, como sucede en las redes tradicionales. Además de la mejora en el desempeño, el retardo entre estaciones extremas se torna más determinístico.

La trama MPOA ofrece un modelo unificado para sobreponer los protocolos de capas entre redes dentro de ATM. Mientras los vendedores implementarán diferentes sabores o aspectos físicos de la trama MPOA, las especificaciones aseguran interoperabilidad entre los diferentes vendedores. El concepto general envuelve funciones de enrutamiento y desvío tradicionalmente soportadas dentro de enrutadores multi-protocolo convencionales entre clientes MPOA y servidores MPOA. El manejo de direcciones y el descubrimiento de topologías, por ejemplo, son desarrolladas por el servidor MPOA (MPS), mientras que el desvío de tráfico es proveído por los clientes MPOA (MPC's) a través de ATM. El MPS reside típicamente en un enrutador conmutado de ATM o en un servidor stand-abone de ATM, mientras que los MPC’s residen en los dispositivos de borde y en los hosts de ATM. Esto provee una separación física de los dispositivos que calculan la ruta entre redes y aquellos que desvían los datos. Como resultado, mientras los enrutadores tradicionales están limitados por la velocidad de sus back-planes propietarios, los sistemas que usan productos basados en enrutamiento con MPOA como los switches ATM resultan en una infraestructura de enrutamiento de multi-gigabit que es idealmente implementada para suplir todas las necesidades asociadas entre redes LAN y WAN.

Ya que los servicios de transporte son ofrecidos sobre infraestructuras basadas en estándares ATM mediante el mapeo de protocolos de red por capas tales IP e IPX directamente a ATM, esto permite que sean desarrollados mecanismos QoS para IP, tales como RSVP [19]. El resultado final es que el tráfico sensible al tiempo puede utilizar las capacidades de QoS de una infraestructura de ATM usando las fortalezas de tecnologías ya instaladas de bajo costo, como Ethernet y TCP/IP en los sitios de trabajo. Con esto se logra aplicaciones multimedia de alto desempeño como video conferencia, distribución de video y aprendizaje a distancia.

Fig. 17 Configuración consolidada para una red entera



Como se puede ver en la figura 17, el servidor de MPOA funciona el apilado lleno del encaminamiento que da lugar a una configuración consolidada

para la red entera. Los interruptores, son interruptores basados los estándares que da lugar a un costo altamente escalable, bajo, infraestructura de ATM de la red del alto rendimiento. Los switches se optimizan para la capa de red de la expedición y el tráfico de la capa 2 dando por resultado redes virtuales anchas de la red y router del cero-salto a través de la red de ATM.

4.1.3 Tres elementos básicos

MPOA usa tres técnicas complementarias de formar su capacidad fundamental. Éstos son emulación del LAN, Resolución de protocolo del siguiente salto (NHRP) y el concepto del router virtual. LANE apoya ambientes nativos del LAN sobre la ATM de una manera transparente, mientras que NHRP proporciona los mecanismos para establecer un atajo sobre ATM del backbone basada en la dirección de la capa de red. El router virtuales proporcionan la capacidad de separar funciones entre los varios elementos de la red, que reduce costo y mejora eficacia.

4.1.3.1 LANE

MPOA supera algunas de las limitaciones del funcionamiento y la escalabilidad de redes basadas LANE. Sin embargo, la versión 2 de

LAN es un componente integral de MPOA. LANE se utiliza para las comunicaciones de la intra-subnet, mientras que los router virtual de MPOA proporcionan comunicaciones entre los subnets. Refiera al apéndice para una explicación más detallada de la operación de LANE.

4.1.3.2 NHRP- resolución de protocolo del siguiente salto

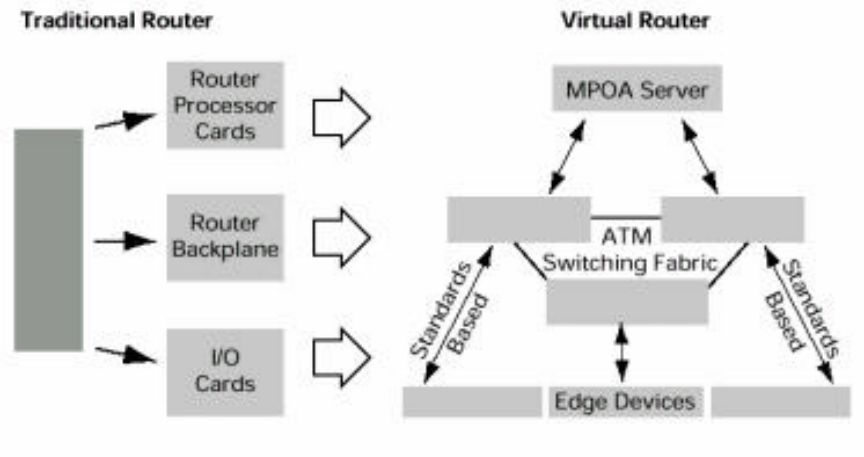
El IETF a definido el protocolo de resolución siguiente salto que entre otras capacidades permite la función de reenvío de paquetes de routers intermedios en el camino de la información que se va a pasar. El NHRP provee

NHRP proporciona un Address Resolution Protocol extendido que permita que los clientes siguientes del salto (NHC's) envíen preguntas entre diversos subnets lógicos del IP (LIS's) designados a veces los grupos locales de la dirección (retrasos). Se propagan las preguntas usando los servidores del salto siguientes (NHS's) a lo largo de las trayectorias descubiertas por protocolos estándares de los routers tales como RIP y OSPF. Esto permite el establecimiento de ATM y SVC's a través de límites del subnet, permitiendo comunicaciones del inter-inter-subnet.

4.1.3.3 Router Virtual

Un router virtual es un conjunto de dispositivos operando sobre una red que colectivamente ofrecen la funcionalidad de las redes enrutadas multiprotocolo. En el caso de MPOA, los dispositivos de borde son análogos para las tarjetas interfaces de enrutamiento; el switcheo de ATM puede ser visto como el “backplane” del enrutador; el servidor MPOA es análogo para el procesador de control. La trama MPOA define los protocolos entre el servidor MPOA y los dispositivos de borde que habilitan el comportamiento como “enrutador virtual”.

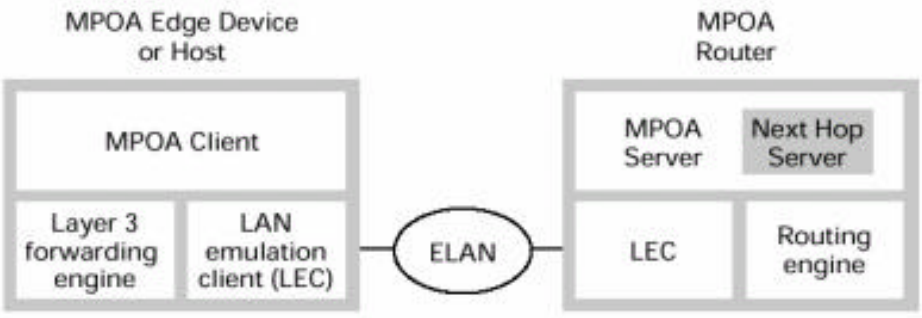
Fig. 18 Enrutador virtual



4.1.4 Componentes Lógicos

MPOA define los componentes lógicos que pueden ser implementados en diversas configuraciones de hardware. La separación de la función permite a los vendedores empacar sus soluciones para satisfacer las necesidades particulares de sus clientes.

Fig. 19 Componentes Logicos



Dispositivos de borde

Los dispositivos de borde [20] no son costosos y son los que desvían los paquetes entre los segmentos de LAN y las interfaces ATM basados en la dirección de la capa de red de destino y la dirección de la capa MAC.

Cliente MPOA—MPC

Los MPC's residen en el dispositivo de borde o en los Hosts ATM anexos y su función principal es la de actuar como un punto de entrada y salida para el tráfico usando los "caminos abreviados" o shortcuts entre redes. Un MPC busca flujos de tráfico, y cuando los encuentra, solicita a su servidor MPS que le provea información del destino y así verificar que el "shortcut" es aceptable. Si lo es, el MPC establece una SVC y desvía los datos a su destino a través del camino. El MPC y el MPS se comunican entre sí usando NHRP. El MPC conserva la información que se deriva de su interacción con el MPS. Los SVC's que no están en funcionamiento son desactivados cuando expira una variable temporizada.

Enrutador MPOA

Un enrutador MPOA es una colección de funciones que permiten el mapeo a ATM de subredes de la capa de red. El enrutador MPOA puede ser implementado como un producto autónomo o puede ser construido dentro de enrutadores o switches existentes. Este conserva la información de la capa de red local, la capa MAC y la dirección ATM, además de las tablas de enrutamiento. Los enrutadores MPOA se comunican vía NHRP para

resolver las direcciones de destino de forma que los MPC's puedan establecer los "shortcuts". El motor de enrutamiento ejecuta protocolos de enrutamiento (ej. RIP y OSPF) para comunicar la información de enrutamiento con "enrutadores tradicionales", permitiendo la interoperabilidad entre redes existentes LAN y WAN.

Servidor MPOA—MPS

Un MPS es un componente lógico del enrutador MPOA que ofrece información de desvío de capa 3 a los MPC's. También incluye la función de servidor NHRP (NHS). El MPS interactúa con su función asociada de enrutamiento y su NHS para identificar un camino representado por la dirección destino de ATM y la información de encapsulación de capa 2, lo cual retorna en la respuesta a una solicitud desde el MPC.

CACHING

Ya que es común para los usuarios en un red enrutada tener direcciones externas habituales y repetitivas a las cuales es necesario conectarse, por ejemplo servidores de archivo o destinos corporativos remotos, el dispositivo de borde puede salvar ("resguardar") la información del canal virtual para ser reusada sin tener que resolver la solicitud de dirección para

cada flujo. Esto es un aspecto importante del concepto del MPOA. Un triunfo en el diseño del MPOA es minimizar el número de veces que el dispositivo de borde debe visitar el servidor de enrutamiento para conseguir esta información. De esta forma, el MPC mantiene su propia "caché" de direcciones.

Mucho del esfuerzo del MPOA se orienta a conseguir técnicas efectivas para la administración de la caché, incluyendo la coherencia entre MPC's y MPS's.

Subredes Virtuales

MPOA usa construcciones de capa de red para definir redes "virtuales". Denotan un protocolo de capa 3 y un rango de direcciones. En el caso de IP, pueden ser pensadas como "redes virtuales". El modelo MPOA soporta todos los flujos de datos de las redes LAN existentes, incluyendo las intra-subredes y las inter-subredes.

4.1.5 Como trabaja

El modelo MPOA distribuye enrutamiento a lo largo de los dispositivos de borde y los Hosts ATM anexos con los clientes MPOA, el cual desvía

paquetes, y los servidores MPOA, los cuales suministran la información de enrutamiento. Los MPC examinan la dirección destino de los paquetes recibidos de los segmentos de LAN para realizar la correcta decisión de enrutamiento. Si el paquete va a ser enrutado, este contendrá la dirección de destino MAC de la interfaz de enrutamiento del MPOA. Si es así, el MPC mirará la dirección destino de la capa de red del paquete y resuelve esto a la correcta dirección ATM basado en la información recibida del servidor MPOA o usa la información en su caché. El MPC establecerá una conexión de canal virtual directo con el destino apropiado. Si el paquete es destinado a un Host en la misma subred de manera que este pueda ser puenteado, el MPC usará LANE para resolver la dirección ATM y establecer una conexión de virtual hacia el destino. Si el servidor de MPOA local no conoce la apropiada dirección ATM, se puede propagar la solicitud a otros servidores MPOA o enrutadores usando la funcionalidad NHRP. La dirección ATM de destino del Servidor MPOA puede ser la dirección del host (si el host es ATM-anexo), o la dirección del dispositivo de borde apropiado al cual deben ser desviados los paquetes.

Mapeo de capa de red:

MPOA funciona en la capa de red 3 para reconocer el inicio de una transferencia de datos y responder con una dirección de destino de ruta de red. El atajo SVC es entonces utilizado para reenviar tráfico utilizando

switcheo estándar de capa 2. Con ambas, capacidades de capa 2 y 3, el modelo MPOA abarca ruteo y switcheo:

1) Siendo capaz de rutear y switchear trafico de la capa de red; y 2) también siendo capaz de puentear trafico no enrutable.

El mapeo de capa de red permite que las propiedades QoS de ATM sean utilizadas para aplicaciones de red.

Por ejemplo, el protocolo RSVP de IETF opera en la capa de red, y provee mecanismos para que las aplicaciones reserven calidad particular de servicio. La estructura MPOA permite que las reservaciones de capa 3 sean mapeadas dentro de la fábrica subyacente de ATM.

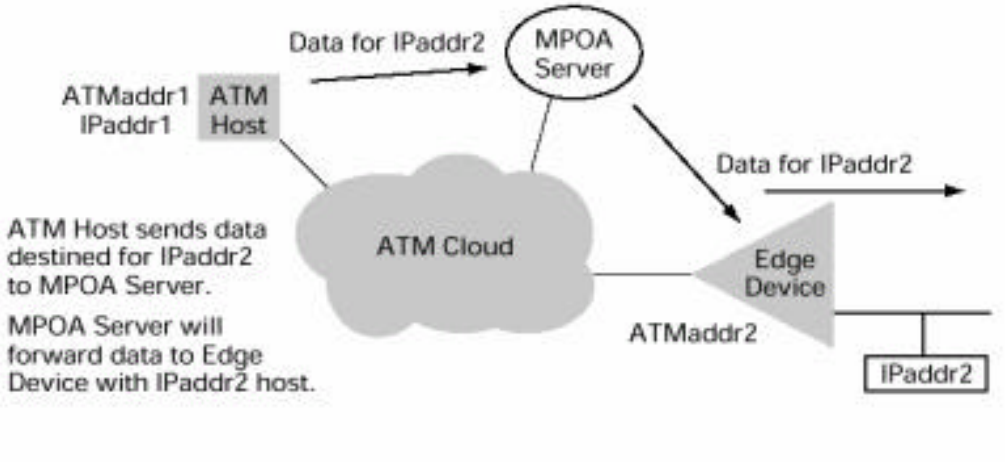
El concepto básico

El concepto fundamental detrás el uso de MPOA para apoyar trafico multiprotocolo LAN-LAN esta basado en el hecho de que, en la mayoría de los casos, la transferencia de datos ocurre en un flujo relativamente constante. Eso es, en archivo o mensaje siendo enviado usualmente consiste en múltiples tramas. Por ejemplo, un archivo de 45K, utilizando un tamaño típico de trama Ethernet de 1500 octetos requeriría como 30

tramas. Como toas las 30 tramas viajarían al mismo destino, es posible identificar el destino y establecer un SVC basado en la información contenida en la primera trama. Entonces todas las 30 tramas podrían ser fraccionadas en aproximadamente 900 células ATM y transmitidas sobre el canal virtual establecido por el SVC. Esto podría considerarse un atajo en el que el flujo completo de datos sigue un camino preestablecido, evitando el camino predeterminado por el trafico ruteado, y mejorando enormemente el desempeño. En el caso de transmisiones de corriente constante tales como video, es altamente eficiente y superior a la simple operación de router a router.

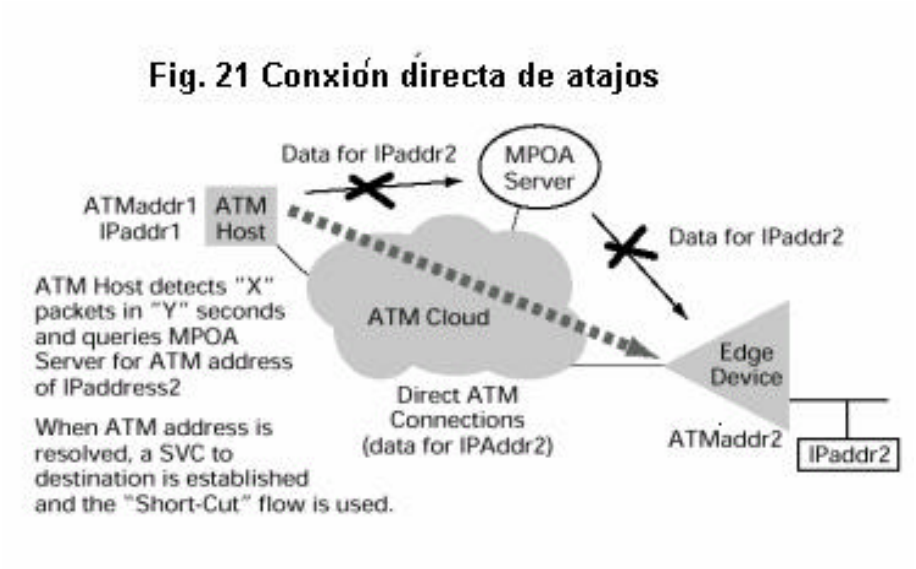
Lo siguiente describe la interacción de los MPC con el MPS:

Fig. 20 Operación básica de MPOA



La figura 20 ilustra la operación básica del MPOA. La primera vez que el tráfico necesita ser reenviado desde un Host ATM con dirección IP de Ipaddr1, el tráfico es reenviado al servidor MPOA. Mientras que se reenvía este trafico, el servidor MPOA capta los mapeos tanto de la dirección IP-a-MAC como la dirección MAC-a-IP.

Fig. 21 Conxión directa de atajos



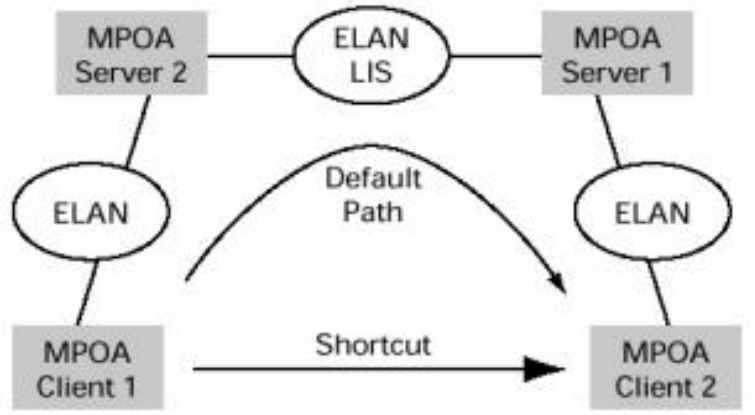
Como se muestra en la figura 21, para establecer una conexión directa de atajo, los MPC obtienen la dirección ATM del punto de salida al cual esta conectada el host de destino. El host de destino es un host con una dirección de capa de red que esta o conectada a una LAN de legado o es una adjunta ATM. Si es un host conectado a una LAN legado tal como una

Ethernet o Token Ring, el MPS devuelve la dirección ATM del dispositivo de borde que corresponde a su dirección de capa de red.

“la vida de un paquete en un día”

A continuación se describe los acontecimientos que permiten que un paquete sea enviado a través de una red de MPOA usando las capacidades del atajo del sistema de MPOA.

Fig. 22 Paquete enviado a través de una red MPOA



Un paquete integra al sistema de MPOA por el MPC (cliente MPOA en la figura 8). Por el defecto, el paquete es punteado sobre vía LANE al enruteador por defecto (ubicado con MPS 2). Desde hay es enrutado por

un MPS 2 hacia el dispositivo de borde de destino. Sin embargo, si este paquete es parte de un flujo para el cual se ha establecido un atajo, el ingreso MPC pela la encapsulación de la capa 2 del paquete y la envía vía a través del Shortcut

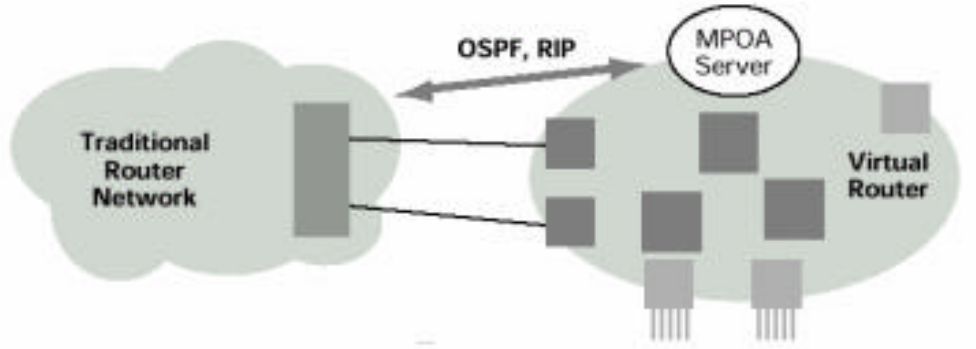
Si no se detectan flujo de datos, cada paquete que es enviado a un MPS es ajustado por su destino de capa 3 y es enviado por LANE. Cuando se excede (los paquetes de "N" a una dirección específica de la capa 3 dentro del tiempo de "X"), el MPC envía una petición de la resolución de MPOA al MPS de obtener la dirección de la ATM para ser usada en establecer un shortcut a la salida (salida) MPC.

Migración y coexistencias

La comunicación MPS con routers externos con protocolos estándares de enrutamiento, como el RIP y OSPF. Esto permite una parecida integración con sistemas sin MPOA y con tráfico calificado sin abreviaturas.

Es importante notar que los dispositivos de enrutamiento en la arquitectura MPOA proveen todas las funciones de un router, incluyendo conexiones de Internet y a través de redes de área extensa, verificación de la integridad, y priorización de la ruta.

Fig. 23 Coexistencias y migración



LAN y MPOA

Mientras que las especificaciones de MPOA se ponen en ejecución para superar algunas de las limitaciones del funcionamiento y de la escalabilidad de las especificaciones de LANE, la versión 2 de LANE es un componente integral de MPOA. La operación del defecto para un dispositivo de MPOA es la conectividad estándar de LANE.

NHRP y MPOA

Puesto que NHRP es un componente integral del servidor de MPOA, una red basada MPOA puede obrar recíprocamente con los router que apoyan funcionalidad de NHRP para propagar peticiones del address resolución de ATM.

4.1.6 Ventajas y desventajas

Ventajas

• Solución para entornos locales/corporativos basados en ATM.

–Libera a los routers de carga en entornos VLAN.

–Servidores no necesitan pertenecer a todas las VLAN’s

Desventajas

• No trabaja con multicast inter-ELAN.

• Posibles problemas de escalabilidad.

–Número de SVC's necesarios elevado.

–Carga de CPU y tiempo de establecimiento de SVC’s.

–Varias aplicaciones TCP/IP no desean un VC dedicado frente a la sobrecarga de establecimiento del mismo.

Capítulo 5

Análisis Técnico económico y relación costo beneficio

5.1.1 La gestión financiera del proyecto

Para el desarrollo del presente proyecto se requería de una inversión en tiempo y dinero tal como lo demostramos en las líneas que siguen. Se trabajo bajo un esquema de análisis técnico económico para fijar un patrón de relación costo beneficio que demuestre no solo la inversión que debe hacerse, sino su ganancia en dinero y valor agregado.

Para reflejar los aspectos relacionados directamente con el dinero, se identificaron los recursos a utilizar y sus costos; en cuanto al valor agregado se fijó una relación en función del daño social y económico de la nación en función del valor del dinero.

5.1.3 Relación costo beneficio

Es difícil establecer la relación costo beneficio cuando no se dispone de valores fijos de comparación, sobre todo por que no sabemos cuanto capital mueve el proceso de integración de la tecnología IP sobre ATM. Sin embargo es posible fijar la atención en la ganancia de valor agregado que se encuentra asociada a la implementación de esta plataforma. Existen compañías tales como siemens que tienen un fondo Los proveedores de servicios han invertido miles de millones de dólares en su actual infraestructura de conmutación de circuitos. ¿Lograrán convencerlos las bondades del softswitch para evolucionar sus redes a la siguiente generación?.

FUERZAS DEL MERCADO

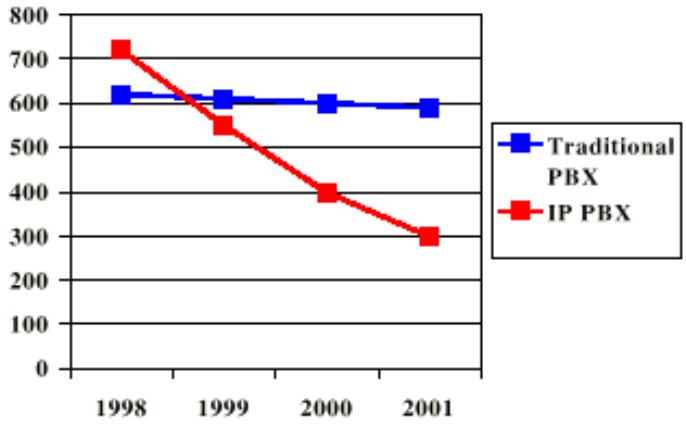
Existe una serie de fuerzas que impulsan la penetración de la tecnología **IP sobre ATM** al interior de una corporación. Estas fuerzas tienen diversos orígenes y van evolucionando de acuerdo a los cambios del mercado. Entre las más

importantes se cuentan.

Ahorros de larga distancia: Inicialmente, el mayor incentivo para desplegar sistemas de telefonía IP (uso de gateways y teléfonos IP) provendrá del ahorro obtenido por cursar llamadas telefónicas sobre la infraestructura de red IP propia o a través de Internet.

Competencia y nuevas aplicaciones: La convergencia de las redes de voz y de datos sobre un protocolo común facilitará a las corporaciones el desarrollo de aplicaciones adaptadas a sus propias necesidades. Un ejemplo de lo anterior son los softwares orientados al objeto que permiten a los clientes crear sus propias aplicaciones de voz.

Reducción de costos de capital: Dado el escaso nivel de innovación tecnológica en el mercado de las PBX tradicionales y considerando la masificación de la tecnología IP y la dinámica de desarrollo tecnológico en el mercado de las redes de datos, se espera que las PBX IP tengan un costo menor que las PBX tradicionales el año 1999. En el siguiente gráfico se muestra la tendencia esperada.



Costos de administración: La instalación de PBX IP tiene como beneficio de más largo plazo una sensible reducción de los costos de administración. Es mucho más barato administrar una infraestructura de red integrada que dos sistemas de red separados e independientes. La definición de características de servicio telefónico más avanzadas pueden ser definidas empleando las mismas herramientas de administración de las redes IP. Un ejemplo de la simplicidad ganada con las redes IP integradas es la conexión de un teléfono al sistema. Sólo es necesario conectarlo a la red para que inmediatamente alcance el estado operacional normal (se emplea el mismo método de reconocimiento que los computadores).

Conectividad de voz sobre aplicaciones de datos: La integración telefonía-datos es un impulso definitivo para servicios avanzados de cliente. Aplicaciones actuales tales como centros de llamada, sistemas de respuesta interactiva y

correos de voz son susceptibles de ser potenciadas e integradas a la red IP corporativa. El interfaz al cliente puede ser dado a través de aplicaciones en el web corporativo.

Nuevas opciones de banda ancha: Las emergentes tecnologías de acceso de banda ancha (ADSL/XDSL y módem de cable) serán un decisivo impulsor de la tecnología IP a nivel de usuario residencial. A través de estos accesos será posible concentrar tráfico proveniente de diferentes fuentes en un solo formato: IP. En consecuencia, la penetración en el mercado del hogar de estas nuevas tecnologías permitirá el desarrollo de multimedia IP.

CONCLUSIONES

Como primera y positiva conclusión, se debe destacar que como fruto del trabajo invertido se logró una solución que reunía los requisitos impuestos por las aplicaciones a evaluar en el proyecto, y cuyo funcionamiento y eficiencia fueron satisfactorios. Este trabajo supone una contribución en general al entendimiento de algunas alternativas para proporcionar QoS a servicios IP, aunque aún queda mucho camino hasta lograr una solución genérica.

En cuanto a la integración de tecnologías, se demostró la posibilidad de interoperación entre IP sobre ATM, siendo posible proporcionar calidad de servicio extremo a extremo utilizando el modelo de Servicios Integrados, así como establecer una correspondencia entre el multicast IP y el ATM. Por su parte, IP se ha demostrado suficientemente maduro. Algunas de sus características, como la capacidad de autoconfiguración, se han probado de gran utilidad. Un aspecto importante a destacar es la aparente falta de escalabilidad al utilizar *IntServ* junto con RSVP en redes ATM, que hace suponer que su uso no es indicado en redes grandes (ya se ha dado una indicación del alto número de circuitos necesarios en una sesión multicast con QoS). Se podría pensar en mejorar la escalabilidad de la solución, intentando disminuir el número de circuitos que es necesario mantener, por ejemplo realizando una compartición inteligente de varios flujos del mismo

circuito ATM (para lo que actualmente no existe una solución estandarizada). En cualquier caso, en una red de acceso el número de sesiones a mantener es limitado, y el uso de Servicios Integrados proporciona ventajas en cuanto a flexibilidad a la hora de establecer políticas y estrategias de contabilidad. Además, *IntServ* es el único modelo con el que se puede tener un control total sobre la cantidad de recursos necesarios en cada momento para lograr la QoS requerida, permitiendo un óptimo aprovechamiento de los mismos. Una línea de continuación encaminada a mejorar aún más el aprovechamiento de los recursos es la implementación del servicio de Carga Controlada sobre circuitos ABR, algo que no se realizó en el proyecto por falta de soporte para este tipo de circuitos por parte del proveedor Winsock2 de ATM de que se disponía.

La monografía es la continuación de otros proyectos anteriores, todos ellos van en la línea de desarrollar un sistema de monitorización de bajo costo que dé soporte a la implantación de políticas de uso aceptable (AUP) en el entorno de redes académicas y de investigación. El resultado es un conjunto de procesos para el análisis de tráfico con un conjunto de utilidades que permiten añadir nuevas funcionalidades y modelar las existentes. La definición de las interfaces entre módulos (ficheros de entrada y salida, ficheros de configuración, parametrización y control) permiten adaptar otras aplicaciones (Netramet[10], NetFlow[11]) de forma fácil. El lenguaje de script permite experimentar al administrador del sistema, y decidir el tipo de análisis que desea obtener

automatizando el tratamiento. Los informes finales pueden ser muy heterogéneos, desde clasificaciones del tráfico por tipo de aplicación, por servidor (dirección IP), por dirección de Red, Sistema Autónomo, enlace, grupo de entidades, tipo de entidad, tipo de tráfico, etc. y de distinta granularidad: horarios, diarios, etc.

Las soluciones de la internetworking. En términos de costo y de complejidad, es una solución que permite que las organizaciones construyan las redes de escala grande conectadas junto con ATM, pero con las capacidades completas de routers. Los routers continuarán siendo importantes en arquitecturas de red y será un componente dominante en cualquier solución de la red.

El foro de ATM continúa trabajando en esta parte importante y en el direccionamiento de IP clásico, LANE y MARS hacía (Multicast-Address Resolution Server) para la ayuda del multicast. Está claro que un modelo específico para integrar ATM en redes multi-protocol de hoy está necesitado en una manera que permita que las organizaciones construyan internetworks multi-media, conservando la importante funcionalidad de los routers mientras que permite el uso continuado de Ethernet existente, el token ring, y las infraestructuras de TCP/IP y de SPX/IPX. MPOA integra el LANE y NHRP para preservar las ventajas de la emulación del LAN, mientras que permite el multiprotocolo over ATM de capa de red del network sobre la ATM SVCs sin requerir los routers convencionales en la trayectoria de datos.

MPOA permite la separación física del cálculo y de la expedición, una técnica de la ruta de la capa de red conocida como encaminamiento virtual. Esta separación proporciona un número de ventajas:

- Alto rendimiento y comunicación eficiente del inter-subnet.

- Flexibilidad creciente disminuyendo el número de los dispositivos que se deben configurar para realizar el cálculo de la ruta de la capa de red.

- Scalability creciente reduciendo el número de los dispositivos que participan en el cálculo de la ruta de la capa de red.
- Reduce la Complejidad de los dispositivos del borde eliminando la necesidad de realizar el cálculo de la ruta de la capa de red.

En los ambientes de hoy en los cuales LANs está creciendo en complejidad e importancia, es crítico que haya sistemas eficaces en el lugar para permitir que estas redes funcionen a través de una tele de ATM.

El acercamiento de MPOA tiene significativas ventajas sobre otras alternativas que cambian de la capa 3. Usando routers el excedente una infraestructura cambiada, un sistema basado en MPOA puede procesar y remitir diez de millones de paquetes por segundo.

En lo que respecta a la integración de IP sobre ATM, nunca podremos dar un 'sí' rotundo y sin objeciones a una solución. Lo que deseamos poner de manifiesto es que de todas éstas, la más interesante de cara al futuro es MPLS, y lo consideramos como tal, por su capacidad para asimilar características de las demás soluciones que ya han sido probadas. Por tanto, con vistas a determinar si MPLS puede llegar a convertirse en el estándar para la integración de IP-ATM, decidimos realizar esta experiencia de simulación. Disponemos, así de una herramienta de estudio pormenorizado (y a la vez didáctica) de su funcionamiento e intentar plantear posibles evoluciones de la tecnología que optimicen el proceso de integración de estos dos tipos de tráfico. Esta herramienta tiene un carácter totalmente abierto, y se está trabajando en su mejora y ampliación de capacidades.

NUEVAS TECNOLOGÍAS

El crecimiento imparable de la Internet, así como la demanda sostenida de nuevos y más sofisticados servicios, supone cambios tecnológicos fundamentales respecto a las prácticas habituales desarrolladas a mitad de los años 90. Nuevas tecnologías de transmisión sobre fibra óptica, tales como Dense Wavelength Division Multiplexing (DWDM), proporcionan una eficaz alternativa al ATM para multiplexar múltiples servicios sobre circuitos individuales. Además, los tradicionales conmutadores ATM están siendo desplazados por una nueva generación de routers con funciones especializadas en el transporte de paquetes en el núcleo de las redes. Esta situación se complementa con una nueva arquitectura de red de reciente aparición, conocida como Multi-Prototocol Label Switching (MPLS). MPLS se considera fundamental en la construcción de los nuevos cimientos para la Internet del próximo siglo. Esta presentación describe las características de MPLS, así como las nuevas posibilidades que abre en la prestación de servicios en un entorno superior de garantías respecto a lo que conocemos hasta ahora.

En la primera parte de la ponencia se analiza la evolución del routing en la Internet desde mitad de los 90 y las motivaciones que han llevado a la adopción del estándar MPLS. Se aprovecha esta introducción para avanzar un aspecto fundamental del MPLS, que consiste en la clara separación entre las funciones de

routing (es decir el control de la información sobre la topología y tráfico en la red), de las funciones de forwarding (es decir el envío en sí de datos entre elementos de la red).

La segunda parte de la ponencia se centra en la descripción funcional del MPLS, de los principales componentes que intervienen en esta arquitectura y de la actuación conjunta de los mismos. A continuación se pasa a discutir las ventajas de MPLS para el soporte de procedimientos de encaminamiento y envío de paquetes en backbones IP, y la posibilidad de proporcionar nuevas aplicaciones y servicios, en redes IP y en la Internet en general. En concreto, se presenta la utilidad del MPLS para el soporte de aplicaciones de: ingeniería de tráfico, de diferenciación de servicios en distintas clases (CoS) y de establecimiento de redes privadas virtuales (VPNs) sobre una topología "inteligente", muy superior en prestaciones a las soluciones tradicionales de túneles y circuitos virtuales.

Palabras clave: IP, ATM, MPLS, encaminamiento, conmutación, intercambio de etiquetas, Calidad de Servicio (QoS), Clases de Servicio (CoS), ingeniería de tráfico, redes privadas virtuales

Este artículo es una reproducción de la ponencia presentada al "Congreso Mundo Internet 2000", Congreso Nacional de Usuarios de Internet e Intranet, Madrid 2-5 febrero 2000.

1- Introducción

Uno de los factores de éxito de la Internet actual está en la acepción de los protocolos TCP/IP como estándar de facto para todo tipo de servicios y aplicaciones. La Internet ha desplazado a las tradicionales redes de datos y ha llegado a ser el modelo de red pública del siglo XXI. Pero si bien es cierto que la Internet puede llegar a consolidarse como el modelo de red pública de datos a gran escala, también lo es que no llega a satisfacer ahora todos los requisitos de los usuarios, principalmente los de aquellos de entornos corporativos, que necesitan la red para el soporte de aplicaciones críticas. Una carencia fundamental de la Internet es la imposibilidad de seleccionar diferentes niveles de servicio para los distintos tipos de aplicaciones de usuario. La Internet se valora más por el servicio de acceso y distribución de contenidos que por el servicio de transporte de datos, conocido como de "best-effort". Si el modelo Internet ha de consolidarse como la red de datos del próximo milenio, se necesita introducir cambios tecnológicos fundamentales, que permitan ir más allá del nivel best-effort y puedan proporcionar una respuesta más determinística y menos aleatoria.

Junto a los últimos avances tecnológicos en transmisión por fibra óptica (principalmente DWDM), que lleva a conseguir anchos de banda de magnitudes muy superiores, y en tecnología de integración de circuitos ASIC (Application Specific Integrated Circuits), que permite aumentar enormemente la velocidad de proceso de información en la red, hemos de considerar la arquitectura MPLS,

sustrato para la inclusión en la red de nuevas aplicaciones y para poder ofrecer diferentes niveles de servicio, en un entorno de mayor fiabilidad y con las necesarias garantías.

MPLS es un estándar emergente del IETF que surgió para consensuar diferentes soluciones de conmutación multinivel, propuestas por distintos fabricantes a mitad de los 90. Como concepto, MPLS es a veces un tanto difícil de explicar. Como protocolo es bastante sencillo, pero las implicaciones que supone su implementación real son enormemente complejas. Según el énfasis (o interés) que se ponga a la hora de explicar sus características y utilidad, MPLS se puede presentar como un sustituto de la conocida arquitectura IP sobre ATM. También como un protocolo para hacer túneles (sustituyendo a las técnicas habituales de "tunneling"). O bien, como una técnica para acelerar el encaminamiento de paquetes... incluso, ¿para eliminar por completo el routing? En realidad, MPLS hace un poco de todo eso, ya que integra sin discontinuidades los niveles 2 (transporte) y 3 (red), combinando eficazmente las funciones de control del routing con la simplicidad y rapidez de la conmutación de nivel 2.

Pero, ante todo y sobre todo, debemos considerar MPLS como el avance más reciente en la evolución de las tecnologías de routing y forwarding en las redes IP, lo que implica una evolución en la manera de construir y gestionar estas redes, las redes IP que queremos ver en el próximo milenio. Los problemas que presentan las soluciones actuales de IP sobre ATM, tales como la expansión sobre una topología virtual superpuesta, así como la complejidad de gestión de dos redes

separadas y tecnológicamente diferentes, quedan resueltos con MPLS. Al combinar en uno solo lo mejor de cada nivel (la inteligencia del routing con la rapidez del switching), MPLS ofrece nuevas posibilidades en la gestión de backbones, así como en la provisión de nuevos servicios de valor añadido. Para poder entender mejor las ventajas de la solución MPLS, vale la pena revisar antes los esfuerzos anteriores de integración de los niveles 2 y 3 que han llevado finalmente a la adopción del estándar MPLS.

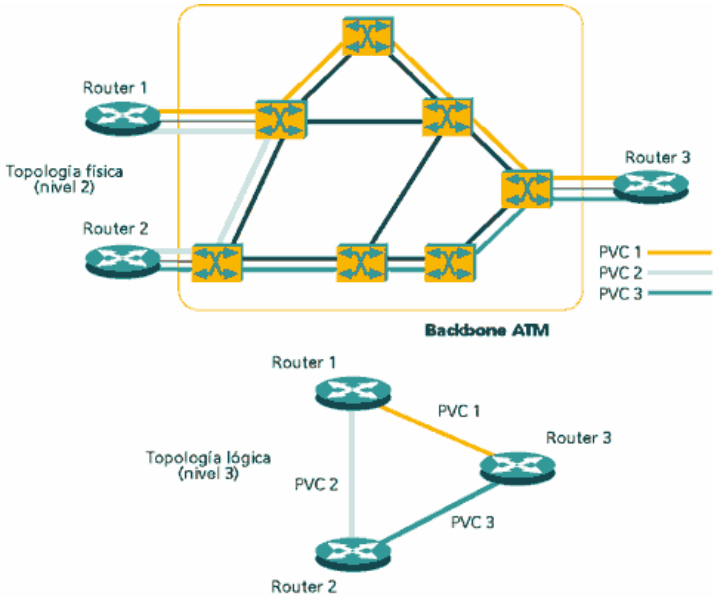
2- El camino hacia la convergencia de niveles: IP sobre ATM

A mediados de los 90 IP fue ganando terreno como protocolo de red a otras arquitecturas en uso (SNA, IPX, AppleTalk, OSI...). Por otro lado, hay que recordar que los backbones IP que los proveedores de servicio (NSP)[2] habían empezado a desplegar en esos años estaban construidos a base de routers conectados por líneas dedicadas T1/E1 y T3/E3. El crecimiento explosivo de la Internet había generado un déficit de ancho de banda en aquel esquema de enlaces individuales. La respuesta de los NSPs fue el incremento del número de enlaces y de la capacidad de los mismos. Del mismo modo, los NSPs se plantearon la necesidad de aprovechar mejor los recursos de red existentes, sobre todo la utilización eficaz del ancho de banda de todos los enlaces. Con los protocolos habituales de encaminamiento (basados en métricas del menor número de saltos), ese aprovechamiento del ancho de banda global no resultaba efectivo. Había que idear otras alternativas de ingeniería de tráfico.

Como consecuencia, se impulsaron los esfuerzos para poder aumentar el rendimiento de los routers tradicionales. Estos esfuerzos trataban de combinar, de diversas maneras, la eficacia y la rentabilidad de los conmutadores ATM con las capacidades de control de los routers IP. A favor de integrar los niveles 2 y 3 estaba el hecho de las infraestructuras de redes ATM que estaban desplegando los operadores de telecomunicación. Estas redes ofrecían entonces (1995-97) una buena solución a los problemas de crecimiento de los NSPs. Por un lado, proporcionaba mayores velocidades (155 Mpbs) y, por otro, las características de respuesta determinísticas de los circuitos virtuales ATM posibilitaban la implementación de soluciones de ingeniería de tráfico. El modelo de red "IP sobre ATM" (IP/ATM) pronto ganó adeptos entre la comunidad de NSPs, a la vez que facilitó la entrada de los operadores telefónicos en la provisión de servicios IP y de conexión a la Internet al por mayor.

El funcionamiento IP/ATM supone la superposición de una topología virtual de routers IP sobre una topología real de conmutadores ATM. El backbone ATM se presenta como una nube central (el núcleo) rodeada por los routers de la periferia. Cada router comunica con el resto mediante los circuitos virtuales permanentes (PVCs) que se establecen sobre la topología física de la red ATM. Los PVCs actúan como circuitos lógicos y proporcionan la conectividad necesaria entre los routers de la periferia. Estos, sin embargo, desconocen la topología real de la infraestructura ATM que sustenta los PVCs. Los routers ven los PVCs como enlaces punto a punto entre cada par. En la figura 1 se representa un ejemplo en

el que se puede comparar la diferencia entre la topología física de una red ATM con la de la topología lógica IP superpuesta sobre la anterior.

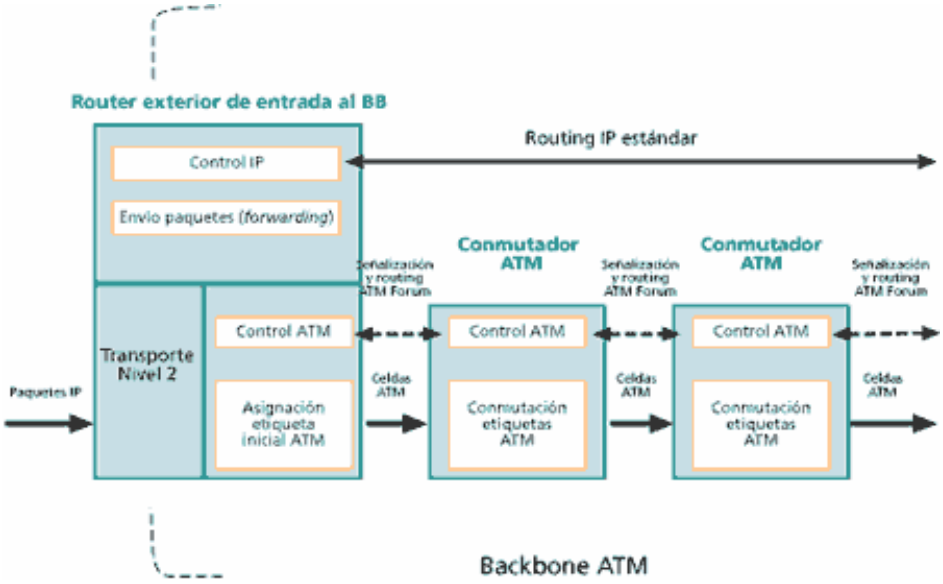


La base del modelo IP/ATM está en la funcionalidad proporcionada por el nivel ATM, es decir, los controles de software (señalización y routing) y el envío de las celdas por hardware (conmutación). En realidad, los PVCs se establecen a base de intercambiar etiquetas en cada conmutador de la red, de modo que la asociación de etiquetas entre todos los elementos ATM determina los correspondientes PVCs. (Más adelante se verá que el intercambio de etiquetas es uno de los componentes fundamentales en la arquitectura MPLS). Las etiquetas tienen solamente significado local en los conmutadores y son la base de la rapidez en la conmutación de celdas. La potencia de esta solución de topologías superpuestas

está en la infraestructura ATM del backbone; el papel de los routers IP queda relegado a la periferia, que, a mitad de los 90, tenían una calidad cuestionable, al estar basados en funcionamiento por software. En la figura 2 se representa el modelo IP/ATM con la separación de funciones entre lo que es routing IP en el nivel 3 (control y envío de paquetes) y lo que es conmutación en el nivel 2 (control/señalización y envío de celdas). Aunque se trata de una misma infraestructura física, en realidad existen dos redes separadas, con diferentes tecnologías, con diferente funcionamiento y, lo que quizás es más sorprendente, concebidas para dos finalidades totalmente distintas.

La solución de superponer IP sobre ATM permite aprovechar la infraestructura ATM existente. Las ventajas inmediatas son el ancho de banda disponible a precios competitivos y la rapidez de transporte de datos que proporcionan los conmutadores. En los casos de NSPs de primer nivel (la mayor parte telcos), ellos poseen y operan el backbone ATM al servicio de sus redes IP. Los caminos físicos de los PVCs se calculan a partir de la necesidades del tráfico IP, utilizando la clase de servicio ATM UBR (Unspecified Bit Rate), ya que en este caso el ATM se utiliza solamente como infraestructura de transporte de alta velocidad (no hay necesidad de apoyarse en los mecanismos inherentes del ATM para control de la congestión y clases de servicio). La ingeniería de tráfico se hace a base de proporcionar a los routers los PVCs necesarios, con una topología lógica entre routers totalmente mallada. El "punto de encuentro" entre la red IP y la ATM está en el acoplamiento

de los subinterfaces en los routers con los PVCs, a través de los cuales se intercambian los routers la información de encaminamiento correspondiente al protocolo interno IGP. Lo habitual es que, entre cada par de routers, haya un PVC principal y otro de respaldo, que entra automáticamente en funcionamiento cuando falla el principal.



Sin embargo, el modelo IP/ATM tiene también sus inconvenientes: hay que gestionar dos redes diferentes, una infraestructura ATM y una red lógica IP superpuesta, lo que supone a los proveedores de servicio unos mayores costes de gestión global de sus redes. Existe, además, lo que se llama la "tasa impuesta por la celda", un overhead aproximado del 20% que causa el transporte de datagramas IP sobre las celdas ATM y que reduce en ese mismo porcentaje el

ancho de banda disponible. Por otro lado, la solución IP/ATM presenta los típicos problemas de crecimiento exponencial n x (n-1) al aumentar el número de nodos IP sobre una topología completamente mallada. Piénsese, Ej., En una red con 5 routers externos con una topología virtual totalmente mallada sobre una red ATM. Son necesarios 5 x 4 =20 PVCs (uno en cada sentido de transmisión). Si se añade un sexto router se necesitan 10 PVCs más para mantener la misma estructura (6 x 5=30). Una pega adicional del crecimiento exponencial de rutas es el mayor esfuerzo que tiene que hacer el correspondiente protocolo IGP.

Como conclusión, podemos decir que el modelo IP/ATM, si bien presenta ventajas evidentes en la integración de los niveles 2 y 3, lo hace de modo discontinuo, a base de mantener dos redes separadas. El MPLS, tal como se verá en las secciones siguientes, logra esa integración de niveles sin discontinuidades.

3- Un paso más en la convergencia hacia IP: conmutación IP

La convergencia continuada hacia IP de todas las aplicaciones existentes, junto a los problemas de rendimiento derivados de la solución IP/ATM, llevaron posteriormente (1997-98) a que varios fabricantes desarrollasen técnicas para realizar la integración de niveles de forma efectiva, sin las discontinuidades señalas anteriormente. Esas técnicas se conocieron como "conmutación IP" (IP

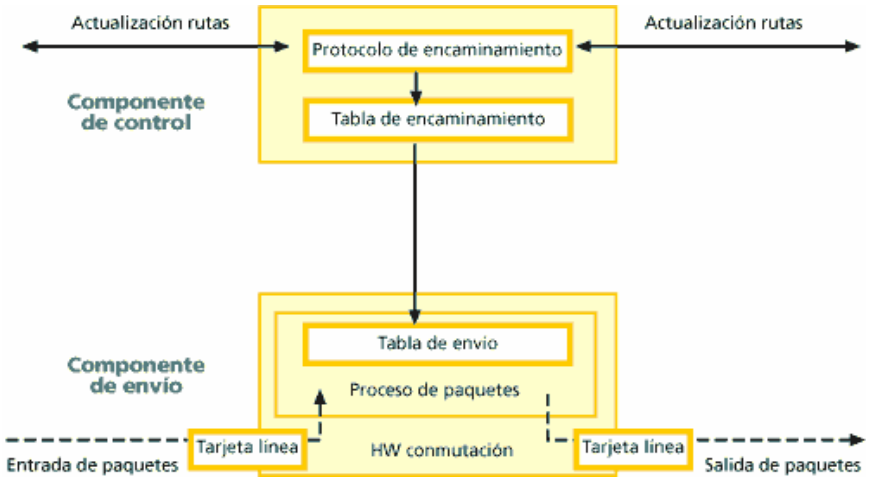
switching) o "conmutación multinivel" (multilayer switching). Una serie de tecnologías privadas -entre las que merecen citarse: IP Switching de Ipsilon Networks, Tag Switching de Cisco, Aggregate Route-Base IP Switching (ARIS) de IBM, IP Navigator de Cascade/Ascend/Lucent y Cell Switching Router (CSR) de Toshiba-condujeron finalmente a la adopción del actual estándar MPLS del IETF. El problema que presentaban tales soluciones era la falta de interoperatividad, ya que usaban diferentes tecnologías privadas para combinar la conmutación de nivel 2 con el encaminamiento IP (nivel 3). Se resume a continuación los fundamentos de esas soluciones integradoras, ya que permitirá luego comprender mejor la esencia de la solución MPLS.

Todas las soluciones de conmutación multinivel (incluido MPLS) se basan en dos componentes básicos comunes:

- la separación entre las funciones de control (routing) y de envío (forwarding)
- el paradigma de intercambio de etiquetas para el envío de datos

En la figura 3 se representa la separación funcional de esas dos componentes, una de control y la otra de envío. La componente de control utiliza los protocolos estándar de encaminamiento (OSPF, IS-IS y BGP-4) para el intercambio de información con los otros routers para la construcción y el mantenimiento de las tablas de encaminamiento. Al llegar los paquetes, la componente de envío busca en la tabla de envío, que mantiene la componente de control, para tomar la

decisión de encaminamiento para cada paquete. En concreto, la componente de envío examina la información de la cabecera del paquete, busca en la tabla de envío la entrada correspondiente y dirige el paquete desde la interfaz de entrada al de salida a través del correspondiente hardware de conmutación.



Al separar la componente de control (encaminamiento) de la componente de envío, cada una de ellas se puede implementar y modificar independientemente. El único requisito es que la componente de encaminamiento mantenga la comunicación con la de envío mediante la tabla de envío de paquetes y actualice la información. El mecanismo de envío se implementa mediante el intercambio de etiquetas, similar a lo visto para ATM. La diferencia está en que ahora lo que se envía por la interfaz física de salida son paquetes "etiquetados". De este modo, se

está integrando realmente en el mismo sistema las funciones de conmutación y de encaminamiento.

En cuanto a la etiqueta que marca cada paquete, decir que es un campo de unos pocos bits, de longitud fija, que se añade a la cabecera del mismo y que identifica una "clase equivalente de envío" (Forwarding Equivalence Class, FEC). Una FEC es un conjunto de paquetes que se envían sobre el mismo camino a través de una red, aun cuando sus destinos finales sean diferentes. Por ejemplo, en el encaminamiento convencional IP por prefijos de red (longest-match) una FEC serían todos los paquetes unicast cuyas direcciones de destino tengan el mismo prefijo. Realmente, una etiqueta es similar a un identificador de conexión (como el VPI/VCI de ATM o el DLCI de Frame Relay). Tiene solamente significado local y, por consiguiente, no modifica la información de la cabecera de los paquetes; tan sólo los encapsula, asignando el tráfico a los correspondientes FEC.

El algoritmo de intercambio de etiquetas permite así la creación de "caminos virtuales" conocidos como LSP (Label-Switched Paths), funcionalmente equivalentes a los PVCs de ATM y Frame Relay. En el fondo, lo que hace es imponer una conectividad entre extremos a una red no conectiva por naturaleza, como son las redes IP, pero todo ello sin perder la visibilidad del nivel de red (de aquí los nombres de conmutación IP o conmutación multinivel). Esta es la

diferencia básica con el modelo IP/ATM. Al hablar de MPLS con más detalle se entenderán mejor estas peculiaridades.

4- La convergencia real: MPLS

Ya se dijo anteriormente que el problema principal que presentaban las diversas soluciones de conmutación multinivel era la falta de interoperatividad entre productos privados de diferentes fabricantes. Además de ello, la mayoría de esas soluciones necesitaban ATM como transporte, pues no podían operar sobre infraestructuras de transmisión mixtas (Frame Relay, PPP, SONET/SDH y LANs). Se quería obtener un estándar que pudiera funcionar sobre cualquier tecnología de transporte de datos en el nivel de enlace. De aquí que el Grupo de Trabajo de MPLS que se estableció en el IETF en 1977 se propuso como objetivo la adopción de un estándar unificado e interoperativo.

4.1. Ideas preconcebidas sobre MPLS

Durante el tiempo en que se ha desarrollado el estándar, se han extendido algunas ideas falsas o inexactas sobre el alcance y objetivos de MPLS. Hay quien piensa que MPLS se ha desarrollado para ofrecer un estándar a los vendedores

que les permitiese evolucionar los conmutadores ATM a routers de backbone de altas prestaciones. Aunque esta puede haber sido la finalidad original de los desarrollos de conmutación multinivel, los recientes avances en tecnologías de silicio ASIC permite a los routers funcionar con una rapidez similar para la consulta de tablas a las de los conmutadores ATM. Si bien es cierto que MPLS mejora notablemente el rendimiento del mecanismo de envío de paquetes, éste no era el principal objetivo del grupo del IETF. Los objetivos establecidos por ese grupo en la elaboración del estándar eran:

- MPLS debía funcionar sobre cualquier tecnología de transporte, no sólo ATM
- MPLS debía soportar el envío de paquetes tanto unicast como multicast
- MPLS debía ser compatible con el Modelo de Servicios Integrados del IETF, incluyendo el protocolo RSVP
- MPLS debía permitir el crecimiento constante de la Internet
- MPLS debía ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP

También ha habido quien pensó que el MPLS perseguía eliminar totalmente el encaminamiento convencional por prefijos de red. Esta es otra idea falsa y nunca se planteó como objetivo del grupo, ya que el encaminamiento tradicional de nivel 3 siempre sería un requisito en la Internet por los siguientes motivos:

- El filtrado de paquetes en los cortafuegos (FW) de acceso a las LAN corporativas y en los límites de las redes de los NSPs es un requisito fundamental para poder gestionar la red y los servicios con las necesarias garantías de seguridad. Para ello se requiere examinar la información de la cabecera de los paquetes, lo que impide prescindir del uso del nivel 3 en ese tipo de aplicaciones.
- No es probable que los sistemas finales (hosts) implementen MPLS. Necesitan enviar los paquetes a un primer dispositivo de red (nivel 3) que pueda examinar la cabecera del paquete para tomar luego las correspondientes decisiones sobre su envío hasta su destino final. En este primer salto se puede decidir enviarlo por routing convencional o asignar una etiqueta y enviarlo por un LSP.
- Las etiquetas MPLS tienen solamente significado local (es imposible mantener vínculos globales entre etiquetas y hosts en toda la Internet). Esto implica que en algún punto del camino algún dispositivo de nivel 3 debe examinar la cabecera del paquete para determinar con exactitud por dónde lo envía: por routing convencional o entregándolo a un LSR, que lo expedirá por un nuevo LSP.
- Del mismo modo, el último LSR de un LSP debe usar encaminamiento de nivel 3 para entregar el paquete al destino, una vez suprimida la etiqueta, como se verá seguidamente al describir la funcionalidad MPLS.

4.2. Descripción funcional del MPLS

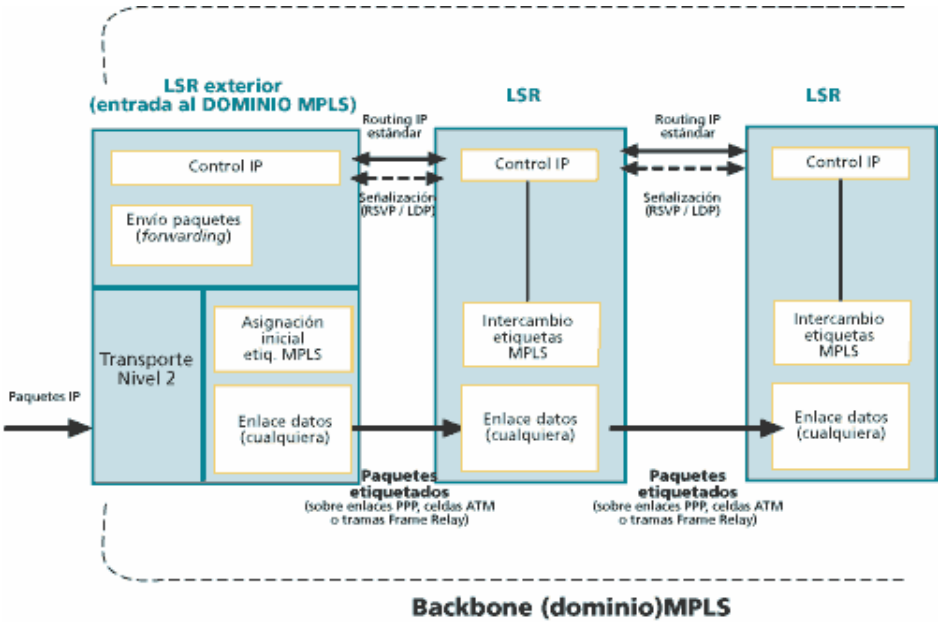
La operación del MPLS se basa en las componentes funcionales de envío y control, aludidas anteriormente, y que actúan ligadas íntimamente entre sí. Empecemos por la primera.

a) Funcionamiento del envío de paquetes en MPLS

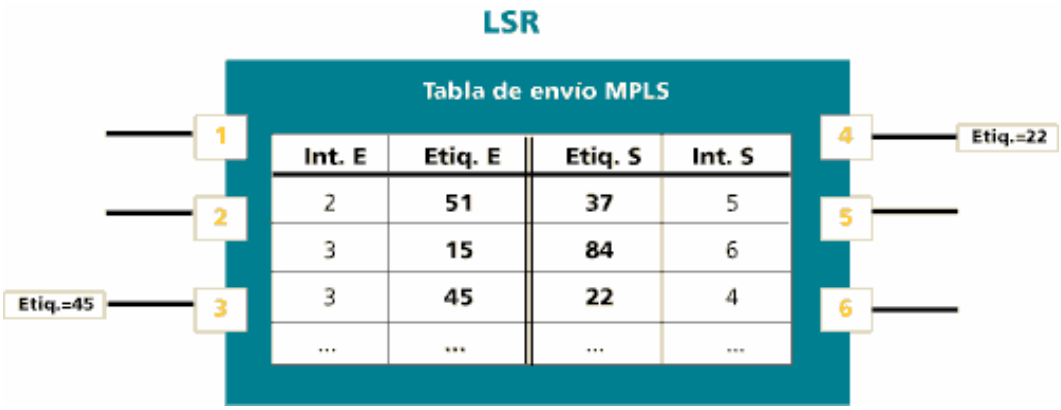
La base del MPLS está en la asignación e intercambio de etiquetas ya expuesto, que permiten el establecimiento de los caminos LSP por la red. Los LSPs son simplex por naturaleza (se establecen para un sentido del tráfico en cada punto de entrada a la red); el tráfico dúplex requiere dos LSPs, uno en cada sentido. Cada LSP se crea a base de concatenar uno o más saltos (hops) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un "conmutador de etiquetas" (Label-Swiching Router) a otro, a través del dominio MPLS. Un LSR no es sino un router especializado en el envío de paquetes etiquetados por MPLS.

En la figura 4 se puede ver la funcionalidad del MPLS. Compárese con los esquemas vistos antes en las figuras 2 y 3 para observar las analogías y diferencias. Al igual que en las soluciones de conmutación multinivel, MPLS separa las dos componentes funcionales de control (routing) y de envío (forwarding). Del mismo modo, el envío se implementa mediante el intercambio de etiquetas en los LSPs. Sin embargo, MPLS no utiliza ninguno de los protocolos de

señalización ni de encaminamiento definidos por el ATM Forum; en lugar de ello, en MPLS o bien se utiliza el protocolo RSVP o bien un nuevo estándar de señalización (el Label Distribution Protocol, LDP, del que se tratará más adelante). Pero, de acuerdo con los requisitos del IETF, el transporte de datos puede ser cualquiera. Si éste fuera ATM, una red IP habilitada para MPLS es ahora mucho más sencilla de gestionar que la solución clásica IP/ATM. Ahora ya no hay que administrar dos arquitecturas diferentes a base de transformar las direcciones IP y las tablas de encaminamiento en las direcciones y el encaminamiento ATM: esto lo resuelve el procedimiento de intercambio de etiquetas MPLS. El papel de ATM queda restringido al mero transporte de datos a base de celdas. Para MPLS esto es indiferente, ya que puede utilizar otros transportes como Frame Relay, o directamente sobre líneas punto a punto.

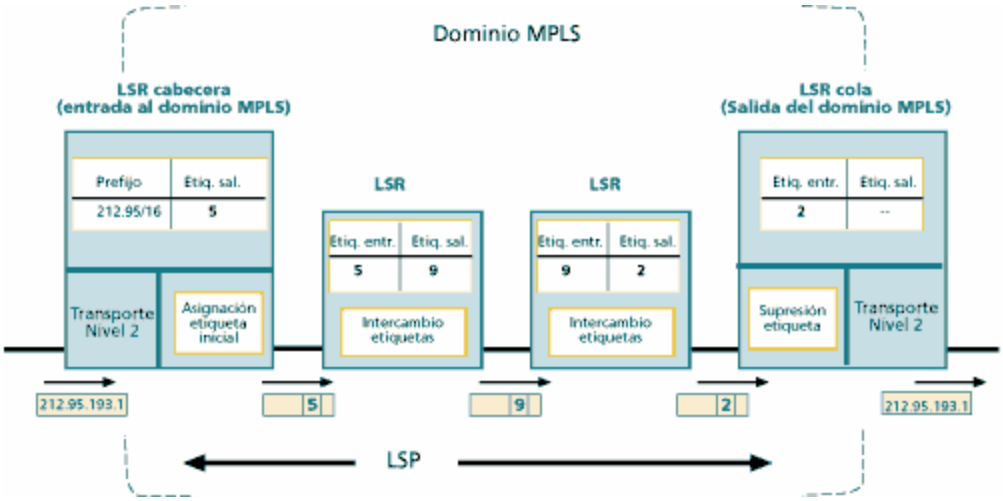


Un camino LSP es el circuito virtual que siguen por la red todos los paquetes asignados a la misma FEC. Al primer LSR que interviene en un LSP se le denomina de entrada o de cabecera y al último se le denomina de salida o de cola. Los dos están en el exterior del dominio MPLS. El resto, entre ambos, son LSRs interiores del dominio MPLS. Un LSR es como un router que funciona a base de intercambiar etiquetas según una tabla de envío. Esta tabla se construye a partir de la información de encaminamiento que proporciona la componente de control (recuérdese el esquema de la figura 3), según se verá más adelante. Cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondientes a cada interfaz de entrada, que se utilizan para acompañar a cada paquete que llega por ese interfaz y con la misma etiqueta (en los LSR exteriores sólo hay una etiqueta, de salida en el de cabecera y de entrada en el de cola). En la figura 5 se ilustra un ejemplo del funcionamiento de un LSR del núcleo MPLS. A un paquete que llega al LSR por el interfaz 3 de entrada con la etiqueta 45 el LSR le asigna la etiqueta 22 y lo envía por el interfaz 4 de salida al siguiente LSR, de acuerdo con la información de la tabla.



El algoritmo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para poder hacer la asignación por el LSR de cabecera. En la figura 6 el LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 212.95.193.1. El LSR consulta la tabla de encaminamiento y asigna el paquete a la clase FEC definida por el grupo 212.95/16. Asimismo, este LSR le asigna una etiqueta (con valor 5 en el ejemplo) y envía el paquete al siguiente LSR del LSP. Dentro del dominio MPLS los LSR ignoran la cabecera IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente (tabla de conmutación de etiquetas) y la reemplazan por otra nueva, de acuerdo con el algoritmo de intercambio de etiquetas. Al llegar el paquete al LSR de cola (salida), ve que el siguiente salto lo saca de la red MPLS;

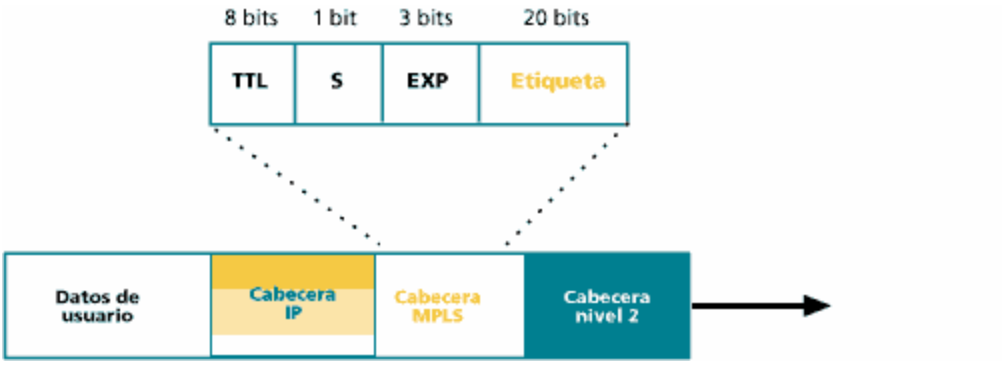
al consultar ahora la tabla de conmutación de etiquetas quita ésta y envía el paquete por routing convencional.



Como se ve, la identidad del paquete original IP queda enmascarada durante el transporte por la red MPLS, que no "mira" sino las etiquetas que necesita para su envío por los diferentes saltos LSR que configuran los caminos LSP. Las etiquetas se insertan en cabeceras MPLS, entre los niveles 2 y 3. Según las especificaciones del IETF, MPLS debía funcionar sobre cualquier tipo de transporte: PPP, LAN, ATM, Frame Relay, etc. Por ello, si el protocolo de transporte de datos contiene ya un campo para etiquetas (como ocurre con los campos VPI/VCI de ATM y DLCI de Frame Relay), se utilizan esos campos nativo para las etiquetas. Sin embargo, si la tecnología de nivel 2 empleada no soporta

un campo para etiquetas Ej. Enlaces PPP o LAN). Entonces se emplea una cabecera genérica MPLS de 4 octetos, que contiene un campo específico para la etiqueta y que se inserta entre la cabecera del nivel 2 y la del paquete (nivel 3).

En la figura 7 se representa el esquema de los campos de la cabecera genérica MPLS y su relación con las cabeceras de los otros niveles. Según se muestra en la figura, los 32 bits de la cabecera MPLS se reparten en: 20 bits para la etiqueta MPLS, 3 bits para identificar la clase de servicio en el campo EXP (experimental, anteriormente llamado CoS), 1 BIT de stack para poder apilar etiquetas de forma jerárquica (S) y 8 bits para indicar el TTL (time-to-live) que sustenta la funcionalidad estándar TTL de las redes IP. De este modo, las cabeceras MPLS permiten cualquier tecnología o combinación de tecnologías de transporte, con la flexibilidad que esto supone para un proveedor IP a la hora de extender su red.



b) Control de la información en MPLS

Hasta ahora se ha visto el mecanismo básico de envío de paquetes a través de los LSPs mediante el procedimiento de intercambio de etiquetas según las tablas de los LSRs. Pero queda por ver dos aspectos fundamentales:

- Cómo se generan las tablas de envío que establecen los LSPs
- Cómo se distribuye la información sobre las etiquetas a los LSRs

El primero de ellos está relacionado con la información que se tiene sobre la red: topología, patrón de tráfico, características de los enlaces, etc. Es la información de control típica de los algoritmos de encaminamiento. MPLS necesita esta información de routing para establecer los caminos virtuales LSPs. Lo más lógico es utilizar la propia información de encaminamiento que manejan los protocolos internos IGP (OSPF, IS-IS, RIP...) para construir las tablas de encaminamiento (recuérdese que los LSR son routers con funcionalidad añadida). Esto es lo que hace MPLS precisamente: para cada "ruta IP" en la red se crea un "camino de etiquetas" a base de concatenar las de entrada/salida en cada tabla de los LSRs; el protocolo interno correspondiente se encarga de pasar la información necesaria.

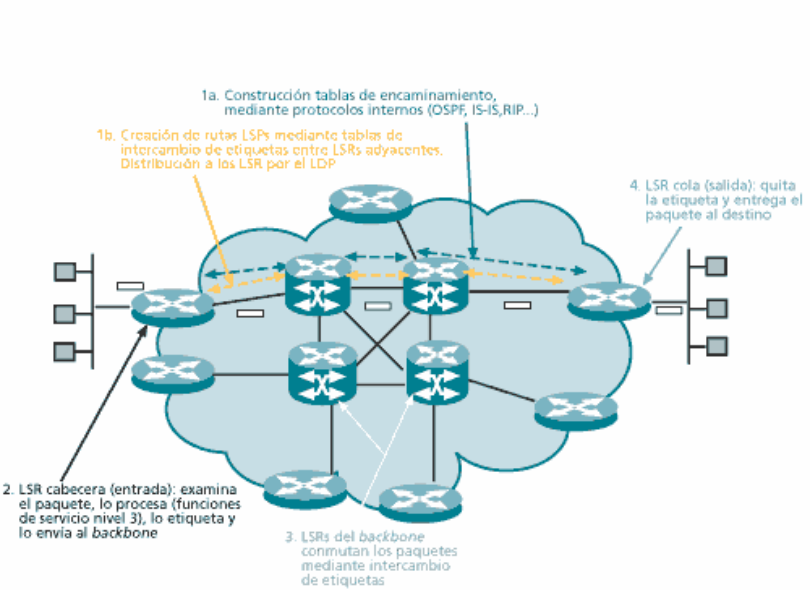
El segundo aspecto se refiere a la información de "señalización" (las comillas se ponen por el impacto que puede suponer este término para los puristas del mundo IP, de naturaleza no conectiva). Pero siempre que se quiera establecer un circuito virtual se necesita algún tipo de señalización para marcar el camino, es decir, para la distribución de etiquetas entre los nodos. Sin embargo, la arquitectura MPLS no

asume un único protocolo de distribución de etiquetas; de hecho se están estandarizando algunos existentes con las correspondientes extensiones; unos de ellos es el protocolo RSVP del Modelo de Servicios Integrados del IETF (recuérdese que ése era uno de los requisitos). Pero, además, en el IETF se están definiendo otros nuevos, específicos para la distribución de etiquetas, cual es el caso del Label Distribution Protocol (LDP). Consúltese las referencias correspondientes del IETF.

c) Funcionamiento global MPLS

Una vez vistos todos los componentes funcionales, el esquema global de funcionamiento es el que se muestra en la figura 8, donde quedan reflejadas las diversas funciones en cada uno de los elementos que integran la red MPLS. Es importante destacar que en el borde de la nube MPLS tenemos una red convencional de routers IP. El núcleo MPLS proporciona una arquitectura de transporte que hace aparecer a cada par de routers a una distancia de un sólo salto. Funcionalmente es como si estuvieran unidos todos en una topología mallada (directamente o por PVCs ATM). Ahora, esa unión a un solo salto se realiza por MPLS mediante los correspondientes LSPs (puede haber más de uno para cada par de routers). La diferencia con topologías conectivas reales es que en MPLS la construcción de caminos virtuales es mucho más flexible y que no se pierde la visibilidad sobre los paquetes IP. Todo ello abre enormes posibilidades a

la hora de mejorar el rendimiento de las redes y de soportar nuevas aplicaciones de usuario, tal como se explica en la sección siguiente.



5-Aplicaciones de MPLS

Las principales aplicaciones que hoy en día tiene MPLS son:

- Ingeniería de tráfico
- Diferenciación de niveles de servicio mediante clases (CoS)
- Servicio de redes privadas virtuales (VPN)

Veamos brevemente las características de estas aplicaciones y las ventajas que MPLS supone para ello frente a otras soluciones tradicionales.

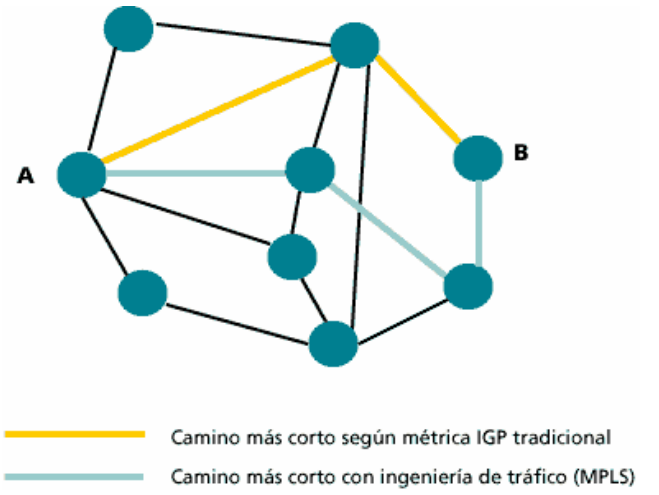
5.1- Ingeniería de tráfico

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén suprautilizados, con posibles puntos calientes y cuellos de botella, mientras otros puedan estar infrautilizados. A comienzos de los 90 los esquemas para adaptar de forma efectiva los flujos de tráfico a la topología física de las redes IP eran bastante rudimentarios. Los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP correspondiente. En casos de congestión de algunos enlaces, el problema se resolvía a base de añadir más capacidad a los enlaces. La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos). En el esquema de la figura 9 se comparan estos dos tipos de rutas para el mismo par de nodos origen-destino.

El camino más corto entre A y B según la métrica normal IGP es el que tiene sólo dos saltos, pero puede que el exceso de tráfico sobre esos enlaces o el esfuerzo de los routers correspondientes haga aconsejable la utilización del camino alternativo indicado con un salto más. MPLS es una herramienta efectiva para esta aplicación en grandes backbones, ya que:

- Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.
- Permite obtener estadísticas de uso LSP, que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos de botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión futura.
- Permite hacer "encaminamiento restringido" (Constraint-based Routing, CBR), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios
- especiales (distintos niveles de calidad). Por ejemplo, con garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.

La ventaja de la ingeniería de tráfico MPLS es que se puede hacer directamente sobre una red IP, al margen de que haya o no una infraestructura ATM por debajo, todo ello de manera más flexible y con menores costes de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.



5.2-Clases de servicio (CoS)

MPLS está diseñado para poder cursar servicios diferenciados, según el Modelo DiffServ del IETF. Este modelo define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades. Según los requisitos de los usuarios, DiffServ permite diferenciar servicios tradicionales tales como el WWW, el correo electrónico o la transferencia de ficheros (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de vídeo y voz interactiva. Para ello se emplea el campo ToS (Type of Service), rebautizado en DiffServ como el octeto DS. (Véase más información sobre el modelo DiffServ

en las referencias correspondientes a QoS). Esta es la técnica QoS de marcar los paquetes que se envían a la red.

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP. De este modo, una red MPLS puede transportar distintas clases de tráfico, ya que:

- el tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP
- Entre cada par de LSR exteriores se pueden provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda. P. Ej., Un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico best-effort, tres niveles de servicio, primera, preferente y turista, que, lógicamente, tendrán distintos precios.

5.3-Redes Privadas Virtuales (VPNs)

Una red privada virtual (VPN) se construye a base de conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de las VPNs es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de

voz, datos y vídeo sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee los enlaces. Las IP VPNs son soluciones de comunicación VPN basada en el protocolo de red IP de la Internet. En esta sección se va a describir brevemente las ventajas que MPLS ofrece para este tipo de redes frente a otras soluciones tradicionales.

Las VPNs tradicionales se han venido construyendo sobre infraestructuras de transmisión compartidas con características implícitas de seguridad y respuesta predeterminada. Tal es el caso de las redes de datos Frame Relay, que permiten establecer PCVs entre los diversos nodos que conforman la VPN. La seguridad y las garantías las proporcionan la separación de tráficos por PVC y el caudal asegurado (CIR). Algo similar se puede hacer con ATM, con diversas clases de garantías. Los inconvenientes de este tipo de solución es que la configuración de las rutas se basa en procedimientos más bien artesanales, al tener que establecer cada PVC entre nodos, con la complejidad que esto supone al proveedor en la gestión (y los mayores costes asociados). Si se quiere tener conectados a todos con todos, en una topología lógica totalmente mallada, añadir un nuevo emplazamiento supone retocar todos los CPEs del cliente y restablecer todos los PVCs. (Algo similar a lo que se vio en la solución IP sobre ATM de la sección 2).

Además, la popularización de las aplicaciones TCP/IP, así como la expansión de las redes de los NSPs, ha llevado a tratar de utilizar estas infraestructuras IP para el soporte de VPNs, tratando de conseguir una mayor flexibilidad en el diseño e

implantación y unos menores costes de gestión y provisión de servicio. La forma de utilizar las infraestructuras IP para servicio VPN (IP VPN) ha sido la de construir túneles IP de diversos modos.

El objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente aparezcan conectados. Lo que se hace es utilizar una estructura no conectiva como IP para simular esas conexiones: una especie de tuberías privadas por las que no puede entrar nadie que no sea miembro de esa IP VPN. No es el objetivo de esta sección una exposición completa de IP VPNs sobre túneles; se pretende tan sólo resumir sus características para poder apreciar luego las ventajas que ofrece MPLS frente a esas soluciones. Se puede obtener más información sobre IP VPN con túneles en las referencias correspondientes a VPNs con MPLS.

Los túneles IP en conexiones dedicadas (no se va a tratar aquí de las conexiones conmutadas de acceso) se pueden establecer de dos maneras:

- en el nivel 3, mediante el protocolo IPSec del IETF
- en el nivel 2, mediante el encapsulamiento de paquetes privados (IP u otros) sobre una red IP pública de un NSP

En las VPNs basadas en túneles IPSec, la seguridad requerida se garantiza mediante el cifrado de la información de los datos y de la cabecera de los paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte por la red del proveedor. Es relativamente sencillo de implementar, bien sea en

dispositivos especializados, tales como cortafuegos, como en los propios routers de acceso del NSP. Además, como es un estándar, IPSec permite crear VPNs a través de redes de distintos NSPs que sigan el estándar IPSec. Pero como el cifrado IPSec oculta las cabeceras de los paquetes originales, las opciones QoS son bastante limitadas, ya que la red no puede distinguir flujos por aplicaciones para asignarles diferentes niveles de servicio. Además, sólo vale para paquetes IP nativos, IPSec no admite otros protocolos.

En los túneles de nivel 2 se encapsulan paquetes multiprotocolo (no necesariamente IP), sobre los datagramas IP de la red del NSP. De este modo, la red del proveedor no pierde la visibilidad IP, por lo que hay mayores posibilidades de QoS para priorizar el tráfico por tipo de aplicación IP. Los clientes VPN pueden mantener su esquema privado de direcciones, estableciendo grupos cerrados de usuarios, si así lo desean. (Además de encapsular los paquetes, se puede cifrar la información por mayor seguridad, pero en este caso limitando las opciones QoS). A diferencia de la opción anterior, la operación de túneles de nivel 2 está condicionada a un único proveedor.

A pesar de las ventajas de los túneles IP sobre los PVCs, ambos enfoques tienen unas características comunes que las hacen menos eficientes frente a la solución MPLS:

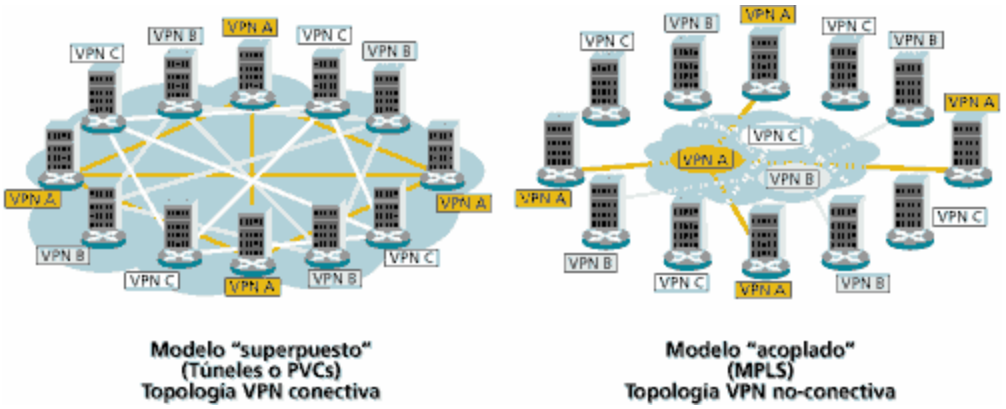
- están basadas en conexiones punto a punto (PVCs o túneles)
- la configuración es manual

- La provisión y gestión son complicadas; una nueva conexión supone alterar todas las configuraciones
- plantean problemas de crecimiento al añadir nuevos túneles o circuitos virtuales
- la gestión de QoS es posible en cierta medida, pero no se puede mantener extremo a extremo a lo largo de la red, ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte

Realmente, el problema que plantean estas IP VPNs es que están basadas en un modelo topológico superpuesto sobre la topología física existente, basándose en túneles extremos a extremo (o circuitos virtuales) entre cada par de routers de cliente en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren añadir nuevos emplazamientos. Con una arquitectura MPLS se obvian estos inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN. Las "nubes" que representan las distintas VPNs se implementan mediante los caminos LSPs creados por el mecanismo de intercambio de etiquetas MPLS. Los LSPs son similares a los túneles en cuanto a que la red transporta los paquetes del usuario (incluyendo las cabeceras) sin

examinar el contenido, a base de encapsularlos sobre otro protocolo. Aquí está la diferencia: en los túneles se utiliza el encaminamiento convencional IP para transportar la información del usuario, mientras que en MPLS esta información se transporta sobre el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de routing IP. Sin embargo, sí se mantiene en todo momento la visibilidad IP hacia el usuario, que no sabe nada de rutas MPLS sino que ve un internet privado (intranet) entre los miembros de su VPN. De este modo, se pueden aplicar técnicas QoS basadas en el examen de la cabecera IP, que la red MPLS podrá propagar hasta el destino, pudiendo así reservar ancho de banda, priorizar aplicaciones, establecer CoS y optimizar los recursos de la red con técnicas de ingeniería de tráfico.

En la figura 10 se representa una comparación entre ambos modelos. La diferencia entre los túneles IP convencionales (o los circuitos virtuales) y los "túneles MPLS" (LSPs) está en que éstos se crean dentro de la red, basándose en LSPs, y no de extremo a extremo a través de la red.



Como resumen, las ventajas que MPLS ofrece para IP VPNs son:

- Proporcionan un modelo "acoplado" o "inteligente", ya que la red MPLS "sabe" de la existencia de VPNs (lo que no ocurre con túneles ni PVCs).
- Evita la complejidad de los túneles y PVCs
- La provisión de servicio es sencilla: una nueva conexión afecta a un solo router
- Tiene mayores opciones de crecimiento modular.
- Permiten mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada.
- Permite aprovechar las posibilidades de ingeniería de tráfico para poder garantizar los parámetros críticos y la respuesta global de la red (ancho

banda, retardo, fluctuación...), lo que es necesario para un servicio completo VPN.

6- Resumen y conclusiones

En el momento actual, todos los NSPs tienen ante sí el enorme reto de gestionar redes cada vez más complejas y extensas, con una mayor gama de servicios y con creciente demanda de ancho de banda, calidad y garantías. Para los backbones, las posibilidades que ofrecen la extensión de infraestructuras de fibra óptica y las nuevas tecnologías de transmisión DWDM son enormes. En este contexto, la evolución natural hacia redes IP y aplicaciones TCP/IP han llevado a desarrollar la arquitectura MPLS como una de las opciones más prometedoras para proporcionar los nuevos servicios del siglo XXI.

MPLS es el último paso en la evolución de las tecnologías de conmutación multinivel (o conmutación IP). La idea básica de separar lo que es el envío de los datos (mediante el algoritmo de intercambio de etiquetas) de los procedimientos de encaminamiento estándar IP, ha llevado a un acercamiento de los niveles 3 y 2, con el consiguiente beneficio en cuanto a rendimiento y flexibilidad de esta arquitectura.

Por otro lado, el hecho de que MPLS pueda funcionar sobre cualquier tecnología de transporte -no sólo sobre infraestructuras ATM- va a facilitar de modo

significativo la migración para la próxima generación de la Internet óptica, en la que se acortará la distancia entre el nivel de red IP y la fibra.

MPLS abre a los proveedores IP la oportunidad de ofrecer nuevos servicios que no son posibles con las técnicas actuales de encaminamiento IP (típicamente limitadas a encaminar por dirección de destino). Además de poder hacer ingeniería de tráfico IP, MPLS permite mantener clases de servicio y soporta con gran eficacia la creación de VPNs. Por todo ello, MPLS aparece ahora como la gran promesa y esperanza para poder mantener el ritmo actual de crecimiento de la Internet.

BIBLIOGRAFÍA

- [1] www.faqs.org/rfcs/rfc1622.html - 35k
- [2] ditec.um.es/laso/docs/tut-tcpip/3376c213.html
- [3] www.solont.com/z-net/tcp-04/tcp_04.htm - 16k
- [4] www.tlmat.unican.es/inteca/inteca/ users/aeg/ryst/Cap3Red/8.htm - 14k
- [5]www.microsoft.com/windows2000/es/advanced/ help/sag_ATM_und_IpAtmComponents.htm - 4k
- [6] www.tlm.unavarra.es/~daniel/docencia/ro/ro02_03/ - 31k
- [7] www.argo.es/~jcea/proyecto/arp.htm - 8k
- [8] www.usr.com/download/datasheets/ broadband/9003/9003-es-ds.pdf –
- [9] www.roper-europe.com/ pagine/prodotti.asp?idcategoria=adsl&lang=spa - 28k
- [10] www.tlmat.unican.es/inteca/inteca/ users/aeg/ryst/Cap3Red/7.htm - 13k
- [11] www.utdallas.edu/~bchen/cs6390/af-mpoa-0087_000.pdf
- [12] www.uwsg.iu.edu/hypermail/linux/ kernel/9603.0/0191.html - 3k
- [13] www.cisco.com/univercd/cc/td/doc/ cisintwk/ito_doc/tokenrng.htm - 22k
- [14] cell.onecall.net/mhonarc/mpls/2000-Jan/msg00186.html - 5k
- [15] www.ldc.usb.ve/~redes/Temas/Tema09/top92.html - 7k - Resultado Suplementario 16

- [16] www.pcredes.com.ar/gratis/diccionario_informatico/ c.htm - 82k - Resultado Suplementario
- [17] COMER, Douglas. Redes globales de información con Internet y TCP/IP. Tercera edición. Mexico 1996. Prentice Hall.
- [18] LAUBACH, M. Classical IP and ARP over ATM. 1994.
- [19]NEWMAN, Peter; GREG, Minshall y THOMAS, Lyon. IEEE ACM Transactions on networking. Vol 6 nº 2. Abril 1998.
- [20] BRAY, Andy. IP over ATM. Octubre 1998.
- LAN Emulation over ATM 1.0" rtf 0021. ATM Forum. Enero 1995..
- "MPOA Baseline". The ATM Forum. RFC 1932. Julio 1995
- "NBMA Next Hop Resolution Protocol (NHRP)" RFC 2332. J. Luciani, D. Katz, D.Piscitello, B.Cole, N.Doraswamy. Abril 1998.

- www.ccaba.upc.es/web/Download/ Papers/TelecomMira2000.pdf

- trevinca.ei.uvigo.es/~adomin/tema4.pdf

- radio-1.ee.dal.ca/~ilow/emerg/pdf/mpoa.pdf

- www.complementos-e.com/pdf/Redes%20LAN%20en%20ambiente%20ATM.pdf

- http://www.telecomsmag.com/issues/199810/tci/bray.html